03 041
YOR

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ３月２８日

出 願 番 号
Application Number: 特願２００３－０９０１３８

[ST. 10/C]: [ＪＰ２００３－０９０１３８]

出 願 人
Applicant(s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００３年１１月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０９５２１３

【書類名】　特許願
【整理番号】　JP9030041
【提出日】　平成15年 3月28日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　青木　義則
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　渡邊　裕治
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　百合山　まどか
【発明者】
　【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
　【氏名】　沼尾　雅之
【特許出願人】
　【識別番号】　390009531
　【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション
【代理人】
　【識別番号】　100086243
　【弁理士】
　【氏名又は名称】　坂口　博

【代理人】
　【識別番号】　100091568
　【弁理士】
　【氏名又は名称】　市位　嘉宏
【代理人】
　【識別番号】　100108501
　【弁理士】
　【氏名又は名称】　上野　剛史
【復代理人】
　【識別番号】　100110607
　【弁理士】
　【氏名又は名称】　間山　進也
【手数料の表示】
　【予納台帳番号】　062651
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9706050
　【包括委任状番号】　9704733
　【包括委任状番号】　0207860
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アクセス管理システム、アクセス管理方法、該アクセス管理方法をコンピュータに実行させるためのコンピュータ実行可能なプログラムおよび該プログラムを記憶したコンピュータ可読な記憶媒体

【特許請求の範囲】

【請求項１】　登録者データへのアクセスを管理するアクセス管理システムであって、該アクセス管理システムは、

登録者のプライバシー・データを含む登録者データを格納した登録者データベースへのアクセスを制御し、かつ、所定のプライバシー・ポリシーと登録者により指定された条件データとを使用して前記登録者データベースへのアクセスを制御する認可エンジンを含み、

前記認可エンジンは、外部から受信するアクセス要求からアクセス型を決定し、かつ前記登録者データについてアクセス型に関連して前記アクセス要求に先立って決定されるアクセス認可データを使用して前記アクセス要求に基づく前記登録者データベースへの参照を制御する認可判断部を含む

アクセス管理システム。

【請求項２】　前記アクセス管理システムは、前記アクセス認可データを事前計算する事前計算部と、前記アクセス認可データを格納する記憶領域を含む、請求項１に記載のアクセス管理システム。

【請求項３】　前記アクセス認可データは、前記プライバシー・ポリシーと前記条件データとから事前に生成されるアクセス認可を行うための識別値を含む、請求項１に記載のアクセス管理システム。

【請求項４】　前記アクセス認可データは、前記プライバシー・ポリシーと前記条件データとを使用して事前に生成され、かつ前記アクセス型または登録者による条件データに応答してアクセスされることのないアクセス認可データを含まない形式のテーブルを含む、請求項２に記載のアクセス管理システム。

【請求項５】　前記アクセス認可データは、さらに認可リストおよび不認可リストを含む請求項４に記載のアクセス管理システム。

【請求項６】　登録者データに対するアクセスをコンピュータ・システムによ

り管理するアクセス管理方法であって、前記アクセス管理方法は、前記コンピュータに対し、

外部からのアクセス要求を前記認可エンジンに対して受信させるステップと、

前記認可エンジンにおいて前記アクセス要求からアクセス型を決定するステップと、

前記登録者データについてアクセス型に関連して前記アクセス要求に先立って決定されるアクセス認可データを読み出して前記アクセス型と比較するステップと、

前記比較に基づいて前記アクセス要求に基づく前記登録者データベースへの参照を制御するステップと

を実行させるアクセス管理方法。

【請求項７】　前記アクセス管理方法は、作成部により生成されたアクセス認可を行うための識別値を含む前記アクセス認可データを記憶領域に格納させるステップを実行させる、請求項６に記載のアクセス管理方法。

【請求項８】　前記アクセス管理方法は、前記プライバシー・ポリシーと前記条件データとを使用して、前記アクセス型または登録者による条件データに応答してアクセスされることのないアクセス認可データを含まないテーブルを含むアクセス認可データを前記記憶領域に格納させるステップを実行させる、請求項６に記載のアクセス管理方法。

【請求項９】　前記アクセス管理方法は、前記アクセス認可データと共に、認可リストおよび不認可リストを前記記憶領域に格納するステップを実行させる、含む請求項８に記載のアクセス管理方法。

【請求項１０】　請求項６～９のいずれか１項に記載のアクセス管理方法を実行させる、コンピュータ実行可能なプログラム。

【請求項１１】　請求項１０に記載のコンピュータ実行可能なプログラムを記憶したコンピュータ可読な記憶媒体。

【請求項１２】　ネットワークを介して登録者データに対するアクセスを管理するためのアクセス管理システムであって、該アクセス管理システムは、

ネットワークと、

前記ネットワークに接続され、登録者のプライバシーを含む登録者データを格納した登録者データベースと、

前記登録者データベースへのアクセス要求を発行するアプリケーション実行部および前記アプリケーション実行部からのアクセス要求を受信し登録者データに対して所定のプライバシー・ポリシーと登録者により指定された条件データとを使用して、前記登録者データベースへのアクセスを制御する前記ネットワークに接続された認可エンジンと、

アクセス型に関連して前記アクセス要求に先立って決定されるアクセス認可データを生成し、前記アクセス認可データを前記認可エンジンに対して使用させるための管理サーバと

を含むアクセス管理システム。

【請求項１３】　前記認可エンジンは、前記プライバシー・ポリシーと前記条件データとを使用し生成され、アクセス認可を行うための識別値を含む前記アクセス認可データを使用して前記アクセスを制御する、請求項１２に記載のアクセス管理システム。

【請求項１４】　前記認可エンジンは、前記プライバシー・ポリシーと前記条件データとを使用して、前記アクセス型または登録者による条件データに応答してアクセスされることのないアクセス認可データを含まない形式とされたテーブルと、かつ認可リストおよび不認可リストとを含んで構成されたアクセス認可データを使用してアクセスを制御する、請求項１２に記載のアクセス管理システム。

【請求項１５】　コンピュータを制御してネットワークを介して登録者データに対するアクセスを管理するためのアクセス管理方法であって、該アクセス管理方法は、コンピュータに対して、

ネットワークを介して前記認可エンジンに事前計算されたアクセス認可データを使用させるステップと、

登録者のプライバシーを含む登録者データを格納した登録者データベースへの外部からのアクセス要求を認可エンジンに対して受信させるステップと、

前記外部からのアクセス要求を受信してアクセス型を決定するステップと、

前記決定されたアクセス型と前記アクセス要求に先立って決定された前記アクセス認可データとを比較して、前記登録者データベースへのアクセスを制御するステップと

を実行させる、ネットワークを介したアクセス制御方法。

【請求項１６】　前記アクセス認可データは、前記プライバシー・ポリシーと前記条件データとを使用して生成され、かつアクセス認可を行うための識別値を含む、請求項１５に記載のアクセス管理方法。

【請求項１７】　前記アクセス認可データは、前記プライバシー・ポリシーと前記条件データとを使用して、前記アクセス型または登録者による条件データに応答してアクセスされることのないアクセス認可データを含まない形式のテーブルと、認可リストおよび不認可リストとを含んで構成される、請求項１５に記載のアクセス管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、機密性の高い個人データを格納するデータベースへのアクセスの管理に関し、より詳細には、個人データといった高度に機密性のあるデータへのアクセスを、高い信頼性で、かつ高速に処理することを可能とする、アクセス管理システム、アクセス管理方法、該アクセス管理方法をコンピュータに対して実行させるためのコンピュータ実行可能なプログラム、および該制御プログラムを記憶したコンピュータ可読な記憶媒体に関する。

【０００２】

さらに本発明は、ネットワークを介して高い機密性を保持させつつ、個人データを格納した登録者データベースへのアクセスを管理するアクセス管理システムおよびアクセス管理方法に関する。

【０００３】

【従来の技術】

近年では、顧客データ、住民データなどの個人データは、データベースに格納されて、保存される場合が多い。とりわけインターネットといったネットワーク

が汎用化されるにつれ、プライバシー・データといった個人データは、１つの管理サイトに設置された登録者データベースに蓄積されてゆくことになる。個人データを膨大な量で記憶したデータベースに対するアクセスは、機密性の高い個人データの不正な漏洩を防止するべく、高いセキュリティ・レベルで管理されなければならず、これまで数多くのアクセス管理手法が提案されてきている。

【０００４】

例えば、企業、自治体、または政府（以下、ポリシー設定者として参照する。）が、顧客、住民、会社、団体（営利、非営利を問わない。以下、単に登録者として参照する。）の登録者データを収集し、データベースに各登録者データを保存する場合を想定する。このとき、データベースに保存されたデータは、プライバシー保護の観点または不正な権利取得といった不正行為の防止といった観点から、高いセキュリティ・レベルにおいて取り扱われる必要がある。

【０００５】

そのため通常では、ポリシー設定者は、収集した登録者データの取り扱いに関する方針をプライバシー・ポリシーとして設定する。このプライバシー・ポリシーには、例えば、収集した登録者データを、誰が、どの情報を、どのような目的で利用するのかについて記述しておくことができる。ポリシー設定者は、登録者データを収集する際に、登録を希望する者に対し、ポリシー設定者が設定したプライバシー・ポリシーを確認することが出来るようにしておき、登録者の同意の下で、そのプライバシー・データを入力させる。ポリシー設定者が、登録者データを取り扱うときには、データベースにアクセスしようとするポリシー設定者側の担当者のアクセス権限をチェックして、該当する登録者データに関するプライバシー・ポリシーを満足しないようなアクセスを排除することにより、登録者データを保護する仕組みを整えておくことが必要とされる。

【０００６】

図１９には、従来プライバシーを考慮することが必要なアクセス管理システムを例示的に示す。図１９では、アプリケーション１００と登録者データベース１０２との間に認可エンジン１０４が配置されている。ポリシー設定者などの担当者は、アプリケーション１００を介して登録者データベース１０２に対してアク

セスする。認可エンジン１０４は、担当者によるアクセス要求を受け付けると、プライバシー・ポリシー・データベース１０６を参照して、担当者のアクセス権限を判断し、担当者がまったく権限判断を受けることなく自由、かつ直接に登録者データベースにアクセスするのを防ぐ構成とされている。図１９に示した認可エンジン１０４の具体的な処理を説明すると、認可エンジン１０４は、アプリケーション１００からの登録者情報へのアクセス要求を受け付けると、アクセス要求がプライバシー・ポリシーを満足しているかを判断する。さらに認可エンジン１０４は、プライバシー・ポリシーを満足していると判断した場合に、登録者データベースへのアクセスを許可して、登録者データの取得を可能とさせ、アプリケーションへと登録者データを返す処理を概ね実行させている。

【０００７】

上述したように、認可エンジン１０４が、アクセス要求を受け付けると実時間でプライバシー・ポリシーを満足しているかを判断することでも、登録者のプライバシー情報が不正に利用されることを防ぐことが可能である。以後、本発明においては、アクセス要求が、プライバシー・ポリシーを満足しているかを検査または判断することを、「適合性チェック」として参照し、その結果、満足していると判断し、アクセス許可を発行することを「認可」として参照する。また、アクセス認可を発行しないこと、またはアクセス不認可信号を発生させることを、「不許可」として参照する。

【０００８】

図１９に示すような認可エンジン１０４を介した登録者データベース１０２へのアクセスは、認可エンジン１０４を使用せずに直接登録者データベース１０２へとアクセスする通常のアクセス管理システムと比較すれば、適合性チェックを行う処理が、アクセス管理システムに付加されることになる。

【０００９】

図２０には、上述したプライバシー・ポリシーの適合性チェックのために使用されるデータおよび処理の具体例を示す。図２０に示す従来のプライバシー・ポリシーの適合性チェックをより具体的に説明するため、図２６では、ポリシー設定者が、ダイレクトメール（ＤＭ）を発送する業務について考察する。ポリシー

設定者は、例えば自己の製品のマーケティングを行うために、マーケティング担当者が、「住所が○○○で、年齢が３０歳以上の登録者」の名前と住所とを登録者データベースから取得しようとするものとする。アプリケーション実行部１００は、「住所が○○○で、年齢が３０歳以上」という条件を、登録者データベース１０２がリレーショナル・データベースであれば、認可エンジン１０４に対し、例えばSQL文という形式でアクセス要求を発行する。このとき、アクセス要求には、SQL文に加えて、適合性チェックに必要な、担当者識別データ（例えば「マーケティング担当者のＡさん」などの実名や、従業員コード、パスワードとユーザＩＤなど）、アクセスしようとしている登録者データの型（例えば、「氏名、住所、電話番号、ＦＡＸ番号」など）、アクセス目的である業務の型（例えば「キャンペーン」）を含ませることができる。

【００１０】

認可エンジン１０４は、アクセス要求を受け取ると、SQL文を実行して、「住所が○○○で、年齢が３０歳以上」という条件を満たす全登録者の「氏名」と「住所」の一覧を受け取る。次に、プライバシー・ポリシー・データベース１０６から、評価の対象とすべき全ポリシーを検索し、ポリシー・データを取得する。次いで、取得した登録者データごとに、以下の手続きを行う。まず、「住所が○○○で、年齢が３０歳以上」という検索で１万件の登録者データがヒットしたとすると、その１万件のレコードの「名前」と「住所」に対して以下の（１）～（２）の計算を実行させる。

【００１１】

（１）評価対象となる全てのプライバシー・ポリシーを評価する。このとき、ポリシーの他に登録者の任意に設定する条件がある場合には、条件判定に必要なデータを取得して、プライバシー・ポリシーの評価を行う。例えば、登録者データベースから同意を記録した条件データを検索し、過去にＤＭの受け取りに同意しているか否かを調べることが必要となる。

【００１２】

（２）評価対象となるすべてのプライバシー・ポリシーの評価結果をもとに、最終的な評価結果を計算する。この、最終的な評価結果を計算する条件データ論

理としては、すべてのポリシーがＯＫだったときのみ認可するＡＮＤ論理や、少なくとも１つはＯＫのポリシーがある場合に認可を行うＯＲロジックなど様々なものが考えられるものの、合計では、（１）および（２）の処理を含めて２万回以下の判断処理を実行することになる。

【００１３】

すなわち、図１９および図２０に示したアクセス管理システムを構成してプライバシー・ポリシーの適合性チェックを行う場合、適合性チェックのための処理に起因するオーバヘッドが問題となる。特に、登録者データベースを用いて行うデータ・マイニングや、キャンペーンの電子メールやＤＭを発送するようなアプリケーションのように、一度に大量の登録者データにアクセスするアプリケーションの場合、そのオーバヘッドが、登録者数の増加につれてますます深刻なオーバヘッドを与え、ポリシー設定者側における業務効率に対して深刻な問題を投げかけることになっていた。

【００１４】

このため、これまで、登録者のプライバシー・データといった高い機密性を有するデータに対して、高い信頼性をもって、かつ高いセキュリティ・レベルのアクセス管理を提供することが必要とされていた。

【００１５】

【発明が解決しようとする課題】

本発明は、上記従来技術の不都合に鑑みてなされたものである。すなわち、本発明によれば、登録者のプライバシー・データといった高い機密性を有するデータに対して、高い信頼性をもって、かつ高いセキュリティ・レベルのアクセスを提供する、アクセス管理システム、アクセス管理方法、該アクセス管理方法をコンピュータに対して実行させるための制御プログラム、および該制御プログラムを記憶したコンピュータ可読な記憶媒体の提供を目的とする。また、本発明は、ネットワークを介して上述したアクセス管理を行うためのアクセス管理システムおよびアクセス管理方法を提供することを目的とする。

【００１６】

【課題を解決するための手段】

上述した目的を達成するために、本発明は、プライバシー・ポリシーがポリシー設定者に依存する要素と、登録者に依存する要素とに分類することができることに着目し、これらの要素を独立したリストまたはテーブルとして構成することにより、アクセス認可データを事前に算出してアクセス認可に適用することができれば、認可エンジンにおける登録者データベースへの適合性チェックを、セキュリティ・レベルを低下させることなく、高速化することができるという着想の下になされたものである。

【００１７】

本発明のアクセス管理方法の第１の実施の形態では、プライバシー・ポリシーのうち、ポリシー設定者に依存する要素を、ポリシー設定者における担当者（データ利用者）のデータ利用型と、業務目的型(business purpose)とを使用して、登録者データベースへのアクセス型を決定し、アクセス認可データとして使用されるアクセス型リストを予め生成して記憶領域に格納しておく。

【００１８】

一方で、登録者に依存する要素は、登録者が設定した任意の数の条件データに基づいて登録者ごとにクラスタ識別値を登録して、アクセス認可データとして使用される登録者条件テーブルを生成する。本発明のアクセス管理方法の第１の実施の形態では、アプリケーションからのアクセス要求を認可エンジンが受け取ると、アクセス型を決定する。認可エンジンは、決定されたアクセス型に基づいて、アクセス型リストを検索し、条件データに対する同意パターンを取得する。この同意パターンをキーとしてアクセス型により認可されるクラスタ識別値を検索する。アクセス認可データにおけるクラスタ識別値の発見は、アクセスの認可を指示し、当該クラスタ識別値に対応する登録者データを登録者データベースから取得し、アプリケーションへと返す構成とされる。さらに、本発明の上述した構成においては、アクセス型リストおよび登録者条件テーブルといったアクセス認可データを、ランタイムにおいてキャッシュ・メモリといった高速アクセス・メモリに逐次更新させることで動的に構築する方法を用いることができる。

【００１９】

また、本発明のアクセス管理方法の第２の実施の形態では、異なる構成のアク

セス認可データを使用する。アクセス認可データは、データ利用型と、業務目的型とを使用して生成されるアクセス型リストを含む。本発明のアクセス管理方法の第２の実施の形態で使用するアクセス認可データは、上述した第１の実施の形態よりもさらに高レベルにポリシー設定者の要素と、登録者側の要素とを機能的に分離したアクセス型リストと登録者条件テーブルを含んで構成される。さらに、本発明のアクセス管理方法において使用されるアクセス認可データは、アクセス型に対応し、アクセス型にそれぞれ付属するアクセス認可データのうち、アクセス型との関連においてアクセスされることのないデータを含まない形式の登録者条件テーブルを含んで構成される。同時に、本発明のアクセス管理方法の第２の実施の形態では、すべてがアクセス認可される認可リストおよびすべてアクセスが不認可とされる不認可リストと共にいわゆる圧縮された登録者条件テーブルを使用することができる。本発明の第２の構成による登録者条件テーブルは、登録者が登録に際して同意した条件に対する所定のルールに基づいて容易に圧縮することが可能であり、高いセキュリティ・レベルを確保しつつ、高速性を付与することを可能とする。

【００２０】

すなわち、本発明によれば、登録者データへのアクセスを管理するアクセス管理システムであって、該アクセス管理システムは、

登録者のプライバシー・データを含む登録者データを格納した登録者データベースへのアクセスを制御し、かつ、所定のプライバシー・ポリシーと登録者により指定された条件データとを使用して前記登録者データベースへのアクセスを制御する認可エンジンを含み、

前記認可エンジンは、外部から受信するアクセス要求からアクセス型を決定し、かつ前記登録者データについてアクセス型に関連して前記アクセス要求に先立って決定されるアクセス認可データを使用して前記アクセス要求に基づく前記登録者データベースへの参照を制御する認可判断部を含む

アクセス管理システムが提供される。

【００２１】

本発明の前記アクセス管理システムは、前記アクセス認可データを事前計算す

る事前計算部と、前記アクセス認可データを格納する記憶領域を含むことができる。本発明の前記アクセス認可データは、前記プライバシー・ポリシーと前記条件データとから事前に生成されるアクセス認可を行うための識別値を含むことができる。

【００２２】

本発明における前記アクセス認可データは、前記プライバシー・ポリシーと前記条件データとを使用して事前に生成され、かつ前記アクセス型または登録者による条件データに応答してアクセスされることのないアクセス認可データを含まない形式のテーブルを含むことができる。本発明の前記アクセス認可データは、さらに認可リストおよび不認可リストを含むことができる。

【００２３】

本発明によれば、登録者データに対するアクセスをコンピュータ・システムにより管理するアクセス管理方法であって、前記アクセス管理方法は、前記コンピュータに対し、

外部からのアクセス要求を前記認可エンジンに対して受信させるステップと、

前記認可エンジンにおいて前記アクセス要求からアクセス型を決定するステップと、

前記登録者データについてアクセス型に関連して前記アクセス要求に先立って決定されるアクセス認可データを読み出して前記アクセス型と比較するステップと、

前記比較に基づいて前記アクセス要求に基づく前記登録者データベースへの参照を制御するステップと

を実行させるアクセス管理方法が提供される。

【００２４】

本発明によれば、上述したアクセス管理方法を実行させる、コンピュータ実行可能なプログラムが提供される。また、本発明においては、上述したコンピュータ実行可能なプログラムを記憶したコンピュータ可読な記憶媒体が提供される。

【００２５】

また、本発明によれば、ネットワークを介して登録者データに対するアクセス

を管理するためのアクセス管理システムであって、該アクセス管理システムは、

ネットワークと、

前記ネットワークに接続され、登録者のプライバシーを含む登録者データを格納した登録者データベースと、

前記登録者データベースへのアクセス要求を発行するアプリケーション実行部および前記アプリケーション実行部からのアクセス要求を受信し登録者データに対して所定のプライバシー・ポリシーと登録者により指定された条件データとを使用して、前記登録者データベースへのアクセスを制御する前記ネットワークに接続された認可エンジンと、

アクセス型に関連して前記アクセス要求に先立って決定されるアクセス認可データを生成し、前記アクセス認可データを前記認可エンジンに対して使用させるための管理サーバと

を含むアクセス管理システムが提供される。

【００２６】

本発明によれば、コンピュータを制御してネットワークを介して登録者データに対するアクセスを管理するためのアクセス管理方法であって、該アクセス管理方法は、コンピュータに対して、

ネットワークを介して前記認可エンジンに事前計算されたアクセス認可データを使用させるステップと、

登録者のプライバシーを含む登録者データを格納した登録者データベースへの外部からのアクセス要求を認可エンジンに対して受信させるステップと、

前記外部からのアクセス要求を受信してアクセス型を決定するステップと、

前記決定されたアクセス型と前記アクセス要求に先立って決定された前記アクセス認可データとを比較して、前記登録者データベースへのアクセスを制御するステップと

を実行させる、ネットワークを介したアクセス制御方法が提供される。

【００２７】

【発明の実施の形態】

セクションＡ：本発明のアクセス管理に使用するアクセス管理データの概説

本発明におけるプライバシー・ポリシーの適合性をチェックするためのシステムとしては、これまで種々知られており、それらの技術は本発明においても利用することができる。より具体的には、本発明の基本的な技術として、”IBM Corporation, IBM Tivoli Privacy Manager for e-business Planning Guide Version 1.1, July 2002”を挙げることができ、本発明において上記文献を参照として含ませることができる。図１には、本発明において、プライバシー・ポリシーとして参照されるデータ構成を示す。図１（ａ）に示すように、プライバシー・ポリシーは、ポリシー設定者側におけるデータ利用者である担当者のデータ利用型１０と、登録者データ型１２と、業務目的型１４と、登録者が設定する条件データ１６とを含んで構成されている。より具体的に説明すれば、データ利用型１０は、マーケティング、物流、課金などの担当者のデータ利用形態を登録するデータである。また、登録者データ型１２は、具体的には住所、氏名、年齢、性別、電話番号、電子メール・アドレスといった登録者のプライバシーを登録したデータであり、業務目的型１４は、より具体的には物流、マーケティング、課金などポリシー設定者側において登録者データにアクセスすることが必要な業務を指定するデータである。条件データ１６は、登録者が、登録を行う際に、登録者のプライバシーにアクセスして良いものとして、登録者が同意して指定した条件を登録したデータである。

【００２８】

各データの構成について例示的に図１（ｂ）を使用して説明する。図１（ｂ）に示すように、ポリシー設定者側において担当者が、物流の業務を処理する担当者であるとする。この場合、担当者は、その業務を遂行するために必要な登録者データ型は、氏名、住所、電話番号が必要とされる。また、物流にも種々の業務フェーズが想定されるものの、図１（ｂ）における「物流」の業務目的型は、発送とされている。図１（ｂ）に示す「物流」の場合には、例えば、プライバシー・ポリシー側で特に条件が設定されていないなどのため、条件データによらず、図１（ｂ）に示した実施の形態では「なし」とされている。一方、担当者のデータ利用型がマーケティングである場合には、ＤＭを送付するための名前と、住所と、郵便番号とが必要とされる。一方で、それ以外の登録者データ型には、アク

セスする必要はない。図１（ｂ）において説明したマーケティングの業務を遂行する場合の業務目的型は、「キャンペーン」であり、この場合の条件データは、登録者によるＤＭ送付への同意となる。

【００２９】

本発明におけるアクセス管理方法では、これらのプライバシー・ポリシーがポリシー設定者に依存して決定される要件と、登録者により指定される要件とに分類できることに着目して、予めアクセス認可データを構成しておき、認可処理を実行させる機能的部分（以下、認可エンジンとして参照する。）が、事前に生成されたアクセス認可データを格納する。アクセス認可データの実施の形態としては、種々想定することができるものの、本発明のアクセス管理方法の第１の実施の形態においては、アクセス認可データを、アクセス型リストと登録者条件テーブルとして作成するものとして説明を行う。

【００３０】

図２は、本発明のアクセス管理方法の第１の実施の形態において作成されるアクセス認可データを構成するアクセス型リストおよび登録者条件リストのデータ構造を示した図である。図２（ａ）には、アクセス型リストの実施の形態を示す。アクセス型リストは、図２（ａ）に示されるように、データ利用型、業務目的型、登録者データ型、および条件データが、それぞれのデータ利用型に対応したレコードとして構成されている。また、図２（ａ）に示されるアクセス型リストは、データ利用型「物流」に対しては、登録者データ型である「住所、氏名」などへのアクセスが、業務目的型「発送」に関しては同意条件が設定されていないなどの理由から、「なし」、すなわちデータ利用型と、業務目的型との組み合わせだけに応答してアクセスできることが示されている。

【００３１】

また、図２（ａ）に示したアクセス型リストにおいては、データ利用型が「課金」の場合では、業務目的型「課金」に関して登録者データ型「住所」へのアクセスが、プライバシー・ポリシーにおいて「不可」、すなわち認可されないことが示されている。さらに、テータ利用型「広報」に対しては、業務目的型「ＤＭ郵送」に関連して、住所、氏名などの登録者データ型へのアクセスが、条件１、

具体的にはＤＭ郵送に対する登録者の同意データを参照して、その返り値を使用すべきことが示されている。図２（ａ）に示したアクセス型リストは、図２（ａ）に示すように通常のテーブル形式で保持させることもできるし、「データ利用型＋登録者データ型＋業務目的型」をキーとしたハッシュテーブルとして保持させておくこともできる。

【００３２】

図２（ｂ）には、本発明におけるアクセス認可データを構成し、図２（ａ）に示したアクセス型リストと共に本発明のアクセス管理システムに含まれる適切な記憶領域に格納される登録者条件テーブルの実施の形態を示した図である。図２（ｂ）に示された登録者条件テーブルには、登録者データベースにおいて登録者ごとに付された登録者識別子（以下、登録者ＩＤとして参照する）と、少なくとも登録者が設定または同意することが必要な条件データのリストと、条件データを、所定の論理、例えば論理和、論理積などを使用して生成されたクラスタ識別値とが、登録者ＩＤごとに登録してレコードを構成している。図２（ｂ）に示した特定の実施の形態では、これら以外の適切な登録者データ型のデータを含んでいてもよい。

【００３３】

図２（ｂ）に示された登録者条件テーブルに登録される条件データとしては、本発明において特に制限を受けるものではないが、例えば氏名の参照、住所の参照、電話番号の参照、ファクシミリ番号の参照、年齢の参照、性別の参照、電子メール・アドレスの参照、興味を持っている分野または嗜好の参照など、プライバシー・ポリシーにおいてポリシー設定者が設定した同意条件に対する同意の有無のデータを挙げることができる。さらにこれ以外にもポリシー設定者が任意に設定することができる、年齢制限といった条件を付加することもできる。図２（ｂ）に示した登録者条件テーブルには、登録者ごとに与えられたクラスタ識別値Ａ～Ｃが与えられている。これ以外のクラスタ識別値であっても本発明においては適宜採用することができる。本発明において登録者条件テーブルに含まれるクラスタ識別値は、該当するクラスタ識別値が発見されただけで、アクセス認可を行うことを可能とする。

【００３４】

また、図２（ｂ）に示した登録者条件テーブルは、予め全体を事前に計算することも可能であるが、後述するように、予め登録領域を確保しておき、ランタイムで条件データの論理判断を実行させ、クラスタ識別値を判定して登録領域のレコードとして追加してゆく実施の形態を使用することができる。さらに、図２（ｃ）には、本発明における図２（ｂ）に示した登録者条件テーブルの機能を、クラスタ識別値をキーとして、同意パターンとそれに対応するクラスタ識別値を格納したテーブルと、登録者ＩＤと、クラスタ識別値とから構成されるテーブルとに分離した構成とした実施の形態を示す。図２（ｃ）に示した実施の形態においても、図２（ｂ）に示したと同様の機能のアクセス認可データを構成することもできる。

【００３５】

図３には、本発明のアクセス管理方法の第１の実施の形態のフローチャートを示す。本発明の第１の実施の形態のアクセス管理方法では、ステップＳ１０において、プライバシー・ポリシー・データベースからプライバシー・ポリシーを読み出して、データ利用型と、認可できる登録者データ型と、業務目的型と、参照すべき条件データとを登録して、アクセス型リストを生成する。ステップＳ１２では、登録者データベースにアクセスして、登録者データ型とそれに対応した条件データとを読み出して、条件データに適用される条件論理に応じて、登録者の同意条件に依存したクラスタ識別値を含む登録者条件テーブルを生成する。

【００３６】

ステップＳ１４では、認可エンジンがアプリケーションからのアクセス要求を受け取り、登録者データベースへのアクセス制御を開始する。ステップＳ１６では、アクセス要求に含まれたポリシー設定者の担当者の要求するデータ利用型と、登録者データ型と、業務目的型とを読み出して、アクセス型リストを検索する。ステップＳ１８では、検索の結果、アクセス型を認可するか否かを判断し、アクセス型がアクセス型リストに含まれている場合(yes)には、ステップＳ２０へと進み、登録者条件テーブルのうちの判断に使用する条件データまたは条件データのセットを取得する。また、ステップＳ２０でアクセス型が認可されないもの

と判断した場合(no)には、ステップＳ２６へと分岐してアプリケーションからのアクセス要求を不認可とする。

【００３７】

ステップＳ２２では、取得された条件データまたは条件データのセットが、予めクラスタ識別値を登録する際の条件データまたは条件データのセットに一致するかを判断して、該当するクラスタ識別値を取得する。ステップＳ２２における比較において、クラスタ識別値が取得されると、ステップＳ２４において登録者条件テーブルを参照して、該当するクラスタ識別値に対応する登録者ＩＤに関して登録者データベースから登録者データを取得させ、アプリケーションに結果を返す。

【００３８】

一方で、ステップＳ２２の判断において、該当するクラスタ識別値が見出されなかった場合(no)には、図３において説明する事前計算を行う本発明の実施の形態においては、ステップＳ２６へと分岐して、登録者データへのアクセス要求を不認可とする。

【００３９】

図４は、図３に示したアクセス管理方法の変更例を示す。図４に示した変更例では、アクセス型リストの作成後、登録者条件テーブルを認可エンジンがランタイムにおいて動的に更新する構成を採用する。図４に示した変更例では、ステップＳ３０において、外部のアプリケーション実行部からのアクセス要求を受け取り、アクセス型を取得する。ステップＳ３２では、取得されたアクセス型がアクセス型リストに含まれるか否かを判断する。ステップＳ３２の判断において、アクセス型がすでに登録されている場合(yes)には、ステップＳ３４で条件データまたは条件データのセットを取得し、ステップＳ３６において登録者条件テーブルを読み出して、条件データの同意パターンを取得し、一致する同意パターンが登録されているか否かを判断する。ステップＳ３６の判断において、一致する同意パターンが見出された場合(yes)には、ステップＳ３８において登録者データベースにアクセスを認可して、該当する登録者データを取得させ、結果をアプリケーションへと返す。

【００４０】

また、ステップＳ３２の判断において、アクセス型に適合するものがないと判断された場合(no)には、ステップＳ４６へと分岐させ、アプリケーションに対してアクセス不認可を通知する。

【００４１】

一方で、ステップＳ３６において、一致する同意パターンが見出されない場合(no)には、処理をステップＳ４２へと進ませ、ステップＳ３４で取得された条件データまたは条件データのセットについて、プライバシー・ポリシーの条件論理をランタイムに適用して従来と同様の適合性チェックを実行させる。ステップＳ４４では、得られた適合性チェックの結果の値を判断し、適合性がある場合(yes)には、ステップＳ４６において、登録者データベースへのアクセスを認可して、該当する登録者データを取得させ、結果をアプリケーションへと返す。同時に、ステップＳ４８においては、新たなクラスタ識別値、例えば「Ｄ」を取得して、登録者条件テーブルに予め生成してあるブランク・レコードに、図２（ｂ）に示したのと同様のデータの書込みを行い、爾後のアクセス要求に高速に対応することができるようにする。

【００４２】

また、ステップＳ４４の判断において適合性がないと判断された場合(no)には、ステップＳ４６へと処理を進ませ、アクセス不認可をアプリケーションへと返す処理を実行させる。本発明の図４において説明した本発明の変更例では、ハードディスクといった記憶媒体に随時登録者条件テーブルやアクセス型リストを書き込むことも可能ではある。しかしながら、本発明のアクセス管理方法の第１の実施の形態では、読み出し・書き込みアクセスをより高速に行うため、ランタイムにアクセス型リストおよび登録者条件テーブルといったアクセス認可データをキャッシュ・メモリにブランク・レコードと共に読み込んで、高速な読み出し・書き込みアクセスを可能とすることもできる。

【００４３】

さらに本発明の他の実施の形態では、アクセス型リストについてもステップＳ４２～ステップＳ４８の処理を適用して、同様の処理を実行させて、アクセス型

リストをランタイムに更新してゆく構成を採用することもできる。

【００４４】

本発明のアクセス管理方法の上述した変更例では、高速メモリにアクセス認可データをクラスタとして登録し、ランタイムに追加・更新を実行する構成を採用する。このため登録されていないアクセス型や、条件データの同意パターンに対しては新たに適合性チェックを実行させることになるものの、（ｉ）予めアクセス型リストや、登録者条件テーブルを構成する処理を実行させずに良い、（ｉｉ）まったく判断されない条件データや、利用度の著しく低いアクセス要求にたいしてまでも適合性チェックの事前計算を行う必要がない、（ｉｉｉ）登録者データの更新があった場合にでも、システムに対して適合性チェックを行うための別の処理プロセスを追加することなく対応することが可能となる。

【００４５】

図５は、本発明のアクセス管理方法において使用されるアクセス認可データの第２の実施の形態を生成するため、プライバシー・ポリシーの再構築例を示した図である。図５に示したプライバシー・ポリシーの再構築例では、図１に示した再構築例よりもさらにポリシー設定者側の要件と登録者側の要件との分離を高度化させるべく再構築を行う。図５に示した実施の形態では、プライバシー・ポリシーから得られるアクセス認可条件を、以下に説明するように再構築する。すなわち、原則的には、データ利用型１０と、業務目的型１４とがポリシー設定者のみにより設定・管理されるものであり、条件データ１６と、登録者データ型１２と、レコード数１８とは、登録者に応じて変更されうるデータである。このため、本発明の第２の実施の形態のアクセス管理方法において使用するアクセス認可データは、データ利用型１０と、業務目的型１４とからアクセス型リストを作成し、さらに、条件データ１６と、登録者データ型１２と、レコード数１８とを使用して、登録者条件テーブルを作成し、これらをアクセス認可データとして事前計算させ、所定の記憶領域に格納させておく構成を採用する。

【００４６】

すなわち、図５に示した本発明のアクセス管理方法においては、アクセス型に対応し、さらに登録者のレコード数の条件データを含む登録者条件テーブルを予

め作成し、登録することになる。図５に示したアクセス認可データを使用したアクセス管理方法では、アクセス型が指定されると、対応する登録者条件テーブルの該当する条件データの値を参照すれば良いだけになるので、ランタイムにプライバシー・ポリシー・データを読み込んで条件論理を適用しながら条件データの適合性をチェックする必要がない点で、従来のアクセス管理方法よりも適合性チェックの処理を高速化させることが可能となるてんでは、本発明の第１の実施の形態のアクセス管理方法と共通する。さらには、図５に示したアクセス管理方法においてもアクセス認可データをランタイムにおいて動的に追加・更新する変更例を採用することができる。

【００４７】

一方で、図５に示したアクセス認可データを使用するアクセス管理方法を実行させる際には、すべてのアクセス型の同意パターンに対して事前計算した登録者条件テーブルを、記憶領域に格納させる必要が生じる。このためには、多くの場合登録者数にしたがって、膨大な記憶領域（メモリ、またはデータベース等）が必要となる。すべてのアクセス型および同意パターンについて事前計算を行うと、理論的には、プライバシー・ポリシーが図１に示す要素で構成される場合、以下の数だけ事前に条件データを使用した計算を実行させ、対応する結果を記憶領域に格納させる必要がある。

【００４８】

【数１】

アクセス型の数　＝「データ利用型」の種類数 ×
「登録者データ型」の種類数 ×
「業務目的型」の種類数 ×
「条件型」の種類数 ×
顧客データベースのレコード数 ……（式1）

【００４９】

使用するアクセス管理システムの記憶容量、処理速度などのハードウエア資源が上述したデータを格納させるに充分な場合には、上述した処理のみでも充分なアクセス管理を行うことが可能である。しかしながら、本発明においては、後述

するように、アクセス型に対応する登録者条件テーブルを圧縮することにより、ハードウエア資源の性能に対して広い適合性を付与することができる。以下、本発明における上述したアクセス認可データの圧縮処理について説明する。本発明における「アクセス認可データの圧縮処理」の用語は、少なくともアクセスに際してプライバシー・ポリシーから判断して、アクセスされることのない登録者条件データを削除し、少なくとも削除された登録者条件データであることを指示する「不認可リスト」を生成する処理を意味するものである。

【００５０】

図６には、本発明のアクセス管理方法において使用することができるアクセス認可データに含まれる登録者条件テーブルの圧縮処理を行う場合の基準軸を示す。本発明においては、登録者条件テーブルは、アクセス型リストのレコードに対応するアクセス型軸と、条件データの数に対応する条件データ軸と、登録者の数に対応する登録者軸の３つの軸を有する３次元構成として捉えることができる。本発明においては、これらの各軸を、圧縮処理における基準軸として使用する。図２に示したプライバシー・ポリシーを検討すると、アクセス型に依存して、まったく利用できないか、利用する必要のない登録者条件テーブルまたは登録者条件データおよび条件を参照するまでもなく、アクセス型の判断のみで適合性チェックを実行することができる場合が存在することがわかる。

【００５１】

具体的には、データ利用型が物流である場合に、業務目的型が課金である場合には、登録者条件テーブルを参照するまでもなく、プライバシー・ポリシーの設定に基づき、条件データ毎の適合性チェックを実行せずともアクセス不認可と判断される。一方で、データ利用型が物流であって、業務目的型が発送である場合には、住所、氏名、電話番号については、ポリシー設定時点でアクセス認可されることがわかっているものもある。また、条件データについてみても、電話によるアクセスは拒否するものの、電子メール、ファックス、ＤＭによるアクセスは許諾するなどの条件データごとの類型パターン、性別、年齢の不必要な利用は拒否するなど登録者ごとの類型パターン、など、登録者の条件データには、一定の類型があることに着目することによって、対応する各基準軸に沿った圧縮処理を

実行させることが可能となる。本発明では、これらを、アクセス型軸での圧縮、条件型軸での圧縮、登録者軸における圧縮処理として参照し、以下にこれらの圧縮処理について詳細に説明する。

【００５２】

＜アクセス型軸における圧縮＞

本発明におけるアクセス型軸とは、具体的にはアクセス型リストのレコードに対応する軸である。この軸に関連した圧縮処理は、アクセス型に関連して適合性チェックを行わずともまったくアクセス認可できない場合、およびすべてアクセスを認可する場合を、作成された登録者条件テーブルのセットから分類し、「認可リスト」および「不認可リスト」に予め登録することによる圧縮処理である。図７は、このための圧縮処理を概略的に示した図である。図７に示すように、データ利用型の数と、業務目的型の数の乗算により与えられるアクセス型１，．．．，アクセス型ｎに対して、それぞれ登録者条件テーブルが構成される。このうち、例えばアクセス型２は、データ利用型が物流であって、業務目的型が課金であるものとすれば、適合性チェックをわざわざ行ったとしてもすべての場合について不認可の判断を与えることとなるので、登録者条件テーブルとしてわざわざ記憶領域に格納させる必要はないので削除することにより圧縮処理を行う。

【００５３】

本発明では、不要な登録者条件型テーブルを削除して、それに対応する不認可リストを構成して圧縮処理を実行させる。図７において説明する実施の形態では、上述したアクセス型２、アクセス型４が不認可リスト２０に加えられている。同時に図７では、アクセス型１およびアクセス型３は、条件データを逐次に判断するまでもなくすべてが認可されるアクセス型として分類できアクセス型１、アクセス型３が認可リスト２２に登録されているのが示されている。例えば、アクセス型１は、データ利用型が「物流」であり、業務目的型が「発送」であって、この場合には、プライバシー・ポリシーは、発送に必要とされる住所、氏名についてはすべての登録者ＩＤについて同意があるので、アクセス要求に含まれる要求登録者データが、住所および氏名である場合には認可判断を都度実行させる必要はないので、認可リストに追加することができる。

【００５４】

さらに、図７には、本発明のアクセス管理方法では、アクセス要求があると、認可エンジンにより、アクセス型を決定し。選択モジュールを使用して、テーブル選択、不認可リストおよび認可リストを参照する処理を行って、適合性チェックを実行することが示されている。

【００５５】

図８には、図７に示したデータ圧縮を使用して本発明のアクセス管理方法を実行させる場合の、認可エンジンが実行する処理を示したフローチャートである。本発明の認可エンジンは、ステップＳ５０において認可エンジンとは別のソフトウエア・モジュールとして構成されたアプリケーションからのアクセス要求を受け取り、データ利用型、業務目的型および要求登録者データの読み取りを実行する。ステップＳ５２では、読み出されたデータ利用型および業務目的型からアクセス型を決定し、ステップＳ５４で、まず不認可リスト２０にアクセスして、取得したアクセス型との比較を実行することにより、不認可リスト２０に決定したアクセス型が登録されているか否かを判断する。ステップＳ５４において、決定されたアクセス型が不認可リスト２０に登録されている場合(yes)には、それ以後の適合性チェックを実行することないので、アプリケーションへとアクセス不認可を発行する。

【００５６】

また、ステップＳ５４の判断により、決定されたアクセス型が不認可リストに登録されていない場合(no)には、条件に応じて、または無条件でアクセスが認可されるのでステップＳ５６へと進んでさらに適合性チェックを実行させる。一方、ステップＳ５４において、不認可リストに取得したアクセス型が登録されている場合には、ステップＳ５８に進んでアプリケーションに対してアクセス不認可を返すことにより、その時点での適合性チェックを終了させる。さらに本発明のアクセス管理方法の他の実施の形態では、最初に認可リスト２２を読み出して、取得したアクセス型が認可リスト２２に登録されていないと判断された時点で、不認可リスト２０を参照させる処理を採用することもできる。

【００５７】

＜条件データ軸における圧縮処理＞

図９には、本発明におけるデータ圧縮法の他の実施の形態である条件データ軸における圧縮処理を示した概略図である。図９に示すように、アクセス型ｉで指定されるアクセス型に対応する登録者条件テーブルでは、すべての登録者が氏名へのアクセスは許諾しているが、住所への該当する業務目的型でのアクセスは同意していないものとする。本発明の条件データ軸に沿った圧縮処理では、カラム単位での認可リスト２４と不認可リスト２６とを作成して、適切な記憶領域に格納させる。同時に、もとの登録者条件テーブルから認可リスト２４および不認可リスト２６に登録されたカラムを削除する。さらに、異なったカラムの条件データを判断して、全登録者が同一のパターンで認可・不認可を登録していないかを判断し、同一のパターンで認可の同意を行っている場合には、カラムを統合し、統合したカラムに対して対応する条件データを参照するインデックスを割り当てる。これらの処理を行ない、最終的には、本発明のアクセス認可データを、｛アクセス型リスト、圧縮された登録者条件テーブル、認可リスト、不認可リスト｝の対として生成させ、認可エンジンが使用できる形式として記憶領域に格納させる。

【００５８】

図１０は、条件データ軸において圧縮処理を実行させたアクセス認可データを使用する場合の、認可エンジンの実行する処理を示したフローチャートである。図１０に示した処理は、ステップＳ６０において、外部機能モジュールとして構成されるアプリケーションからのアクセス要求を受け取り、データ利用型、業務目的型、および要求登録者データとを取得し、アクセス型を決定する。ステップＳ６２では、取得されたアクセス型に対応してアクセス認可データを参照し、認可リストまたは不認可リストを参照する。ステップＳ６４では、要求登録者データに該当するアクセス型が各リストに登録されているか否かを判断し、認可リストおよび不認可リストに該当するアクセス型が登録されている場合(yes)には、ステップＳ６６へと進み、該当するリストにしたがってアクセスを制御する。一方で、ステップＳ６４で認可リストおよび不認可リストにおいて該当するアクセス型が見出されない場合には、ステップＳ６８へと進んで、さらに他の適合性チ

ェックを実行する。

【００５９】

＜登録者軸における圧縮処理＞

図１１には、本発明において使用する登録者軸におけるデータ圧縮処理の概略について説明する。ポリシー設定者が設定するプライバシー・ポリシーにおいては、異なる登録者であっても同一のデータ型に対して一定の類型を有する同一の認可判断を与える場合もある。この場合に、条件データの類型毎に登録者の圧縮を行うことにより、登録者条件テーブルの圧縮を行うことも可能である。具体的には、例えば図１１（ａ）に示されるように、登録者ＩＤが００２と、登録者ＩＤが００４の登録者は、氏名からメールまでの同意条件データが同一であり、類型を形成するものといえる。また同様の処理を、カラム単位で実行させることもできる。図１１（ｂ）には、カラム単位で登録者の認可・不認可リストを示し、図１１（ｃ）には、レコード単位で類型毎に認可・不認可リストを構成させることにより、データの圧縮を実行したリストを示す。図１１に示した登録者軸でのデータ圧縮は、いずれの場合も各リストにはもれなく登録者の認可・不認可データが登録されているので、認可エンジンは、いずれかのリストをルックアップして認可判断を実行する。この実施の形態における認可エンジンの判断処理は、概ね本発明の第１のアクセス認可データを使用するものと概ね同様にして実行させることができる。

【００６０】

また、本発明のアクセス管理方法においても、アクセス認可データは、高速のキャッシュ・メモリにブランク・レコードと共に格納させておき、ランタイムに逐次追加してゆく構成を採用することができる。

【００６１】

図１２には、本発明の第２のアクセス認可データを使用した場合に実行することができる、ランタイムにアクセス認可データを追加・更新する処理のフローチャートを示す。図１２に示したランタイムにおいてアクセス認可データを更新する処理は、ステップＳ８０から開始し、該当するアクセス型に対応する登録者条件テーブルがあるか否かを判断する。ステップＳ８０の判断において、該当する

登録者条件テーブルが存在する場合(yes)には、ステップＳ８２へと進んで、判断しているアクセス型が、認可・不認可リストに登録されているか否かを判断する。

【００６２】

ステップＳ８２の判断において、判断するべきアクセス型が認可・不認可リストに含まれていない場合(no)には、ステップＳ８４へと進んで条件データ軸において生成される認可・不認可リストに登録されているか否かを判断する。認可・不認可リストに登録されていない場合(no)には、ステップＳ８６において、登録者軸において生成されるクラスタが存在するか否かを判断する。ステップＳ８６の判断においても該当するアクセス型が存在しない場合(no)には、ステップＳ８８においてプライバシー・ポリシー・データを読み出して適合性チェックを行い、チェックの結果と登録者ＩＤとをブランクの登録者条件テーブルについてして、処理を終了する。一方で、認可ステップＳ８０の判断において該当する登録者条件テーブルが存在しない場合(no)には、ステップＳ９０において対応する登録者条件テーブルをブランクのまま作成し、記憶領域に格納させ、ステップＳ８２へと処理を分岐させて次の認可判断を実行させる。

【００６３】

また、ステップＳ８２の判断において、認可・不認可リストに属していると判断された場合(yes)には、ステップＳ９２へと進んで、認可・不認可リストと登録者条件テーブルとのコンシステンシをチェックし、ステップＳ８４の判断に分岐する。本発明においてコンシステンシをチェックする処理は、認可・不認可リストを使用して得られたアクセス認可が、登録者条件テーブルにより与えられた結果と矛盾しないかを判断し、矛盾する場合には認可・不認可リストから生成されたアクセス認可を削除して、正しいアクセス認可に修正して格納する処理を意味する。さらに、ステップＳ８４の判断において認可・不認可リストに属していると判断された場合(yes)には、ステップＳ９４へと進んで、認可・不認可リストと登録者条件テーブルとのコンシステンシをチェックし、ステップＳ８６の判断に分岐する。さらに、ステップＳ８６の判断において該当するアクセス型のクラスタがあると判断した場合(yes)には、当該クラスタに対して適合性チェック

を実行した結果を使用して、当該登録者ＩＤを追加し、処理を終了させる。

【００６４】

これまで説明した圧縮処理は、いずれか単独で使用しなければならないというものではなく、上述したように必要に応じて複数組み合わせてデータ圧縮を実行することができる。例えば、アクセス型軸に対して圧縮処理を行った後、条件データ軸について圧縮処理を行い、認可リストまたは不認可リストに含まれなかったカラムについて条件データ軸に対する圧縮処理を行い、その後レコード単位での登録者軸に対する圧縮処理を行うことにより、認可エンジンが、アプリケーションからのアクセス要求を受け取った後に実行する適合性チェックのオーバヘッドを著しく低減させることが可能になる。

【００６５】

Ｂ．本発明のアクセス管理方法の実装

本発明のアクセス管理方法は、コンピュータ実行可能なプログラムとして構成され、コンピュータ可読な記憶媒体または伝送媒体としてコンピュータ・システムに実装されることにより、コンピュータに上述した各機能を達成させることにより実装が行われる。以下、本発明のアクセス管理方法をコンピュータ・システムに対して実装させる場合の処理について説明する。なお、以下の説明では、最も基本的なアクセス管理システムを使用して説明するものの、それぞれネットワークを介して相互接続されるアクセス管理方法またはアクセス管理システムであっても、同様の機能は、適切な構成要素に対して構成することができる。

【００６６】

図１３には、本発明のアクセス管理方法の処理開始までの初期処理(primary processing)を示した図である。この処理は、システムのいずれかのコンピュータに構成された事前計算部により実行することができる。図１３に示した初期処理は、ステップＳ１００において、ポリシー設定者により設定されたプライバシー・ポリシー・データを事前計算部に読み込ませる。この格納方法としては、システムのいずれかの格納部に格納されたプライバシー・ポリシー・データを読み出すことによっても実行することができ、またポリシー設定者のポリシー管理部門の担当者が適切な方法で入力し、格納させることもできる。

【００６７】

ステップＳ１０２では、使用するアクセス認可データの形式に応答してクラスタ識別値生成または圧縮処理のいずれかを実行させて、上述したアクセス型リストおよび登録者条件型テーブルを含むアクセス認可データを作成し、記憶領域に格納させる。このための実施の形態としては、認可エンジンと、作成部とが共用することができるメモリ領域にアクセス型リスト、登録者条件型テーブル、条件論理、選択論理などを格納させることもできる。また、認可エンジンと作成部とがネットワークを介して遠隔的に相互接続された実施の形態では、認可エンジンに対してアクセス型リスト、登録者条件型テーブル、条件論理、選択論理などを転送して認可エンジンに格納させることもできるし、また認可エンジンが作成部におけるアクセス型リスト、登録者条件テーブル、条件論理、選択論理などを参照して処理することもできる。

【００６８】

ステップＳ１０４では、認可エンジンに対して、適合性チェックの処理を開始させ、アプリケーションからのアクセス要求に対応して登録者データベースへのアクセスを管理させる。ステップＳ１０６では、監視部が登録者の同意といった条件型についての変更およびポリシー設定者側でのポリシー内容の変更があるか否かを継続的または周期的にモニタさせる。ステップＳ１０６における判断の結果は、ステップＳ１０８へと送られ、ステップＳ１０８においていずれかのデータが更新されたと判断した場合(yes)には、ステップＳ１１０へと進み、アクセス型リスト、登録者条件型テーブル、条件論理、選択論理などの変更しなければならない部分を特定し、事前計算部において再計算を実行させる。

【００６９】

ステップＳ１１２では、アクセス型リスト、登録者条件型テーブル、条件論理、選択論理などのうち、再計算された部分を認可エンジンが使用可能として適切な記憶領域に格納させ、ステップＳ１０４へと処理を戻してアクセス管理システムの処理を継続的に実行させる。また、ステップＳ１０８の判断の結果、データの更新がないと判断した場合（no)には、従前のアクセス型リスト、登録者条件型テーブル、条件論理、選択論理などはそのまま使用することができるので、ア

クセス認可データの更新を行うことなく、処理をステップＳ１０４へと戻し、アクセス管理システムの処理を実行させる。

【００７０】

図１４には、登録者条件型テーブルを事前に作成しておくのではなく、動的に追加してゆく実施の形態の処理の実施の形態を示す。図１４に示した実施の形態では、ステップＳ１１４において、認可エンジンは、登録者データへのアクセス要求をアプリケーションから受け取り、アクセス型を取得する。ステップＳ１１６において、認可エンジンは、アクセス型リストおよび登録者条件型テーブルを検索し、取得したアクセス型がアクセス認可データにおいて見出されるか否かを判断する。ステップ１１６の判断において、登録者条件型テーブルに該当するデータが見出されない場合(no)には、ステップＳ１１８へと進んで認可エンジンは、アクセス認可データに該当する結果がないこと、および要求されたアクセス型を事前計算部に通知する。ステップＳ１２０では、事前計算部は、登録者データベースへとアクセスしてアクセス型に該当する登録者を抽出し、登録者データをプライバシー・ポリシーと対比させて、適合性チェックを実行させ、クラスタ識別値を生成し、登録者条件型テーブルにおける新たなレコードとして登録する。ステップＳ１２２では、作成部は、生成されたアクセス認可データをその全体または更新された一部を認可エンジンに返し、認可エンジンによる適合性チェックを実行させる。

【００７１】

一方、ステップＳ１１６の判断において登録者条件型テーブルに該当するデータが見出された場合には、すでに適合性チェックを実行させて得られたクラスタ識別値を参照するだけで、その時点で評価しているアクセス要求に対する適合性チェックを完了させることができる。図１４に示した実施の形態は、ランタイムで条件データの適合性チェックを行うため、本発明のアクセス管理方法を適用する当初には、図１４で説明した実施の形態よりもアプリケーション側における結果の受け取りには時間を要するものの、一旦登録者条件型テーブルが構成されてしまえば、図１４において説明したと同一の効率を与えることが可能となる。また、この処理を高速に処理するため、キャッシュ・メモリに登録者条件型テーブ

ルを順次構築することもできる。

【００７２】

図１５は、本発明の第２の実施の形態のアクセス管理方法において、アクセス型ごとに登録者条件テーブルを作成する場合に、動的にレコードを追加する実施の形態の処理を示した図である。図１５においては、ステップＳ１３０において認可エンジンがアプリケーションからの登録者データへのアクセス要求を受け取り、アクセス型を決定する。ステップＳ１３２において、決定されたアクセス型および要求登録者データをキーとして、アクセス型リストを参照し、アクセス型リストに決定されたアクセス型があるか否かを判断する。ステップＳ１３２の判断において、アクセス型リストが見出された場合(yes)には、ステップＳ１３４に進み、該当する登録者条件型テーブルを使用してアクセスの認可判断を実行させ、その結果に基づいてステップＳ１４０において登録者データベースへのアクセス制御を実行させ、ステップＳ１３０へと処理を戻し、次のアクセス要求に備える。

【００７３】

一方、ステップＳ１３２の判断において、アクセス型リストにその時点で判断しているアクセス型が見出されない場合(no)には、ステップＳ１３６へと進み、認可エンジンがアクセス型が見出されない通知および当該アクセス型を作成部に渡す。ステップＳ１３８では、事前計算部は、プライバシー・ポリシー・データを使用して適合性チェックを実行し、適合性チェックの結果と共にアクセス認可データの新たなレコードを作成し、評価エンジンが使用できる形式としてアクセス認可データを記憶領域に格納させる。ステップＳ１４０では、評価エンジンは、新たに取得したレコードを使用して適合性チェックを実行し、その結果をアプリケーションに返すことにより、処理が行われる。

【００７４】

Ｃ．本発明のアクセス管理システム：

図１６には、本発明のアクセス管理方法を実装した本発明のアクセス管理システムの概略的な機能ブロック図を示す。図１６に示すように、本発明のアクセス管理システム３０は、アプリケーション実行部３２からのアクセス要求を受け付

け処理を実行する、認可エンジン３４と、事前計算部３８と、記憶領域４０とを含んで構成されている。認可エンジン３４は、アクセスの認可判断を処理するための認可判断部３６を含んで構成されている。アプリケーション実行部３２は、担当者からの入力を受け付け、アクセス要求をSQL文などを使用して認可エンジン３４に対して発行するとともに、認可エンジンからの結果を受け取って、担当者に返す処理を実行する。アプリケーション実行部３２は、ポリシー設定者が必要とする業務に関連する固有の、または汎用の業務ソフトウエアをコンピュータにより実行させることにより、所定の業務を遂行することができる構成とされている。

【００７５】

認可エンジン３４は、アクセス要求を受け取って、アクセス要求に含まれるデータ利用型、業務目的型、要求登録者データといったデータを読み出し、読み出されたデータから要求されたアクセス型を決定して、ハードディスク、高速アクセス・メモリ（キャッシュ・メモリ）などを含んで適切に構成されるメモリ領域４０に格納する。一方で、事前計算部３８は、プライバシー・ポリシー・データベース４２に格納されたプライバシー・ポリシーと、登録者データベース４４に格納された登録者データとを読み出して、アクセス型リストおよび登録者条件テーブルを含むアクセス認可データを事前に作成する。作成されたアクセス認可データは、例えばメモリ領域４０へと格納される。この場合、メモリ領域４０は、適切なソフトウエアにより構成されるデータベースを含んで構成することもできる。

【００７６】

生成されたアクセス型リストおよび登録者条件テーブルを含むアクセス認可データは、一旦メモリ領域４０へと格納された後、認可エンジン３４により読み出し可能とされている。同時に登録者条件テーブルの選択論理を与えることが必要な場合には、事前計算部３８により、同時にメモリ領域４０へと格納される。

【００７７】

再度、図１６を参照して本発明のアクセス管理システムを説明すると、監視部４６は、アクセス管理システム３０は、プライバシー・ポリシー・データベース

４２および登録者データベース４４のデータの変更または更新を監視している。また、監視部４６は、プライバシー・ポリシー・データベース４２および登録者データベース４４におけるデータのコンシステンシを、例えば定期的に、または継続的にモニタしている。例えば、登録者が条件データに対する設定を変えた場合や、新たな登録者のレコードが追加された場合には、監視部４６は、データの一致しない部分を抽出して条件データの設定変更または登録者レコードの追加を判断する。監視部４６は、条件データの設定変更や、新たな登録者レコードが追加されたと判断した場合には、事前計算部３８へと変更された条件型または新たな登録者データを送る。これらのデータを受け取った事前計算部３８は、これらに対応するアクセス認可データを作成し、認可エンジン３４が新たな登録者データを含んだ処理を実行することができるように、差分データを記憶領域４０に格納させる。

【００７８】

図１７は、本発明のアクセス管理システムの第２の実施の形態を示した図である。本発明のアクセス管理システムの第２の実施の形態は、アクセス型軸、条件データ軸、または登録者軸におけるデータ圧縮を行う場合の構成を示した図である。本発明のアクセス管理システム４８は、認可エンジン３４と、事前計算部３８と、記憶領域４０とを含んで構成されている。認可エンジン３４は、さらに認可判断部３６と、アクセス認可データにおいて各テーブルやリストを選択する判断を実行する選択モジュール４８とを含んで構成されている。アプリケーション実行部３２は、概ね図１６において説明したと同様の処理を実行して、担当者に対してアクセス管理により与えられる結果を返す処理を実行する。

【００７９】

認可エンジン３４は、アクセス要求を受け取って、アクセス要求に含まれるデータ利用型、業務目的型、要求登録者データといったデータを読み出し、読み出されたデータから要求されたアクセス型を決定する。また、事前計算部３８は、プライバシー・ポリシー・データベース４２に格納されたプライバシー・ポリシーと、登録者データベース４４に格納された登録者データとを読み出して、アクセス型リスト、登録者条件テーブルと、それに対応する圧縮データなどを、圧縮

処理により生成された認可・不認可リストやテーブルの参照を可能とさせる選択論理とを作成し、ハードディスク、高速アクセス・メモリ（キャッシュ・メモリ）などを含んで適切に構成されるメモリ領域４０に格納する。

【００８０】

選択モジュール５０は、決定されたアクセス型を受け取り、同時に選択論理およびアクセス認可データを記憶領域４０から読み出して、アクセス認可データを認可判断部へと渡す。認可エンジン３４は、受け取ったアクセス要求およびアクセス認可データを使用して、登録者データベースへのアクセスを認可または不認可の判断を可能している。アクセスが認可された場合には、該当する登録者データへのアプリケーション実行部３２による取得を可能とし、アクセスが認可されない場合には、アプリケーション実行部３２は、認可エンジン３４からのアクセス不認可の通知を受け取る。

【００８１】

図１８は、本発明のアクセス管理システムの第３の実施の形態を示した図である。図１４に示されたアクセス管理システム５０は、ＬＡＮ（ローカルエリア・ネットワーク）またはＷＡＮ（ワイドエリア・ネットワーク）といったネットワークを介して登録者データへとアクセスを管理するシステムである。図１８に示されたアクセス管理システム５０は、ネットワーク５２と、ネットワーク５２に接続された複数のアプリケーション・コンピュータ５４と、登録者データベース４４と、プライバシー・ポリシー・データベース４２とを含んで構成されている。説明している実施の形態においては、登録者データベース４４およびプライバシー・ポリシー・データベース４２は、管理サーバ５６により管理されている。また、管理サーバ５６は、図１６および図１７において説明した事前計算部３８の機能、監視部４６の機能、および記憶領域４０の機能を含んで構成されており、アクセス型リスト、登録者条件テーブル、選択論理など、本発明のアクセス管理方法を実行するために必要なデータなどを事前に算出し、格納しておくことができる構成とされている。一方、図１８に示した実施の形態においては、アプリケーション・コンピュータ５４には、アプリケーション実行部３２と、認可エンジン３４とを含んで構成されている。

【００８２】

図１８に示した認可エンジン３４には、管理サーバ５６から認可判断処理に必要なアクセス管理データが、選択論理のデータとともに伝送されており、アプリケーション・コンピュータ５４に含まれた適切な記憶領域に格納されている。各アプリケーション・コンピュータ４４は、格納されたアクセス認可データと、アクセス要求とを使用して、アプリケーション・コンピュータ６４におけるアクセス要求を処理しており、認可エンジン３４により、登録者データベースへのアクセスが制御される構成とされている。認可エンジン３４は、上述した本発明のアクセス管理方法に基づいてアクセス要求を処理し、適合性チェックをパスしたアクセス要求のみを、管理サーバ５６へと送り、管理サーバ５６は、登録者データベース４２から要求される登録者データを検索・抽出して、アプリケーション・コンピュータ５４へと登録者データを渡している。

【００８３】

また、本発明のさらに他の実施の形態においては、アプリケーション・コンピュータ５４に認可エンジン機能を設けることなく、別に認可サーバ（図示せず）を構成して、管理サーバ５６とは別に、アプリケーション・コンピュータ５４からのアクセス要求を処理するゲートウエイ・サーバとして認可エンジンを構成し、複数のアプリケーション・コンピュータ５４からのアクセス要求を、事前計算機能とは独立して処理させることもできる。

【００８４】

これまで、本発明の図面に示した特定の実施の形態に基づいて説明してきたが、本発明は、説明した特定の実施の形態に限定されるものではない。また、本発明のアクセス管理方法は、種々のプログラミング言語を使用したコンピュータ実行可能なプログラムとして記述することができ、このようなプログラミング言語としては、Ｃ言語、Ｃ＋＋言語、Java（登録商標）などを挙げることができる。また、本発明の音源取得方法を実行させるためのコンピュータ実行可能なプログラムは、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、ＣＤ－ＲＯＭ、ＤＶＤ、フレキシブル・ディスク、ハードディスクなどに格納して頒布することができる。

【００８５】

本発明を適応することにより、プライバシー・ポリシーの適合性チェックを、信頼性を損ねることなく、高速化することが可能となる。特に、一度に大量の情報を取得するようなアプリケーションでは、適合性チェックのオーバヘッドが大きな問題となるが、本発明はそのような大量のデータ・アクセスを伴うシステムにおいて特に有効である。

【図面の簡単な説明】

【図１】　本発明におけるプライバシー・ポリシーとして参照されるデータ構成を示した図。

【図２】　本発明のアクセス管理方法の第１の実施の形態において作成されるアクセス認可データを構成するアクセス型リストおよび登録者条件リストのデータ構造を示した図。

【図３】　本発明のアクセス管理方法の第１の実施の形態のフローチャート。

【図４】　図３に示した本発明の第１の実施の形態のアクセス管理方法の変更例を示した図。

【図５】　本発明のアクセス管理方法において使用されるアクセス認可データの第２の実施の形態を生成するため、プライバシー・ポリシーの再構築例を示した図。

【図６】　本発明のアクセス管理方法において使用することができるアクセス認可データに含まれる登録者条件テーブルの圧縮処理を行う場合の基準軸を示した図。

【図７】　本発明におけるアクセス型軸に沿った圧縮処理を概略的に示した図。

【図８】　図７に示したデータ圧縮を使用して本発明のアクセス管理方法を実行させる場合の、認可エンジンが実行する処理を示したフローチャート。

【図９】　本発明におけるデータ圧縮法の他の実施の形態である条件データ軸における圧縮処理を示した概略図。

【図１０】　条件データ軸において圧縮処理を実行させたアクセス認可データを使用する場合の、認可エンジンの実行する処理を示したフローチャート。

【図１１】　本発明において使用する登録者軸におけるデータ圧縮処理の概略について説明した図。

【図１２】　本発明の第２のアクセス認可データを使用した場合に実行することができる、ランタイムにアクセス認可データを追加・更新する処理のフローチャート。

【図１３】　本発明のアクセス管理方法の処理開始までの初期処理(primary processing)を示したフローチャート。

【図１４】　登録者条件型テーブルを事前に作成しておくのではなく、動的に追加してゆく実施の形態の処理の実施の形態を示した図。

【図１５】　本発明の第２の実施の形態のアクセス管理方法において、アクセス型ごとに登録者条件テーブルを作成する場合に、動的にレコードを追加する実施の形態の処理を示した図。

【図１６】　本発明のアクセス管理方法を実装した本発明のアクセス管理システムの概略的な機能ブロック図。

【図１７】　本発明のアクセス管理システムの第２の実施の形態を示した図。

【図１８】　本発明のアクセス管理システムの第３の実施の形態を示した図。

【図１９】　従来のアクセス管理システムを示した図。

【図２０】　従来のアクセス管理システムにおけるデータフローを示した図。

【符号の説明】

１０…データ利用型

１２…登録者データ型

１４…業務目的型

１６…条件データ

１８…レコード数

２０…不認可リスト

２２…認可リスト

２４…認可リスト

２６…不認可リスト

３０…アクセス管理システム

３２…アプリケーション実行部

３４…認可エンジン

３６…認可判断部

３８…事前計算部

４０…記憶領域

４２…プライバシー・ポリシー・データベース

４４…登録者データベース

４６…監視部

４８…選択モジュール

５０…アクセス管理システム

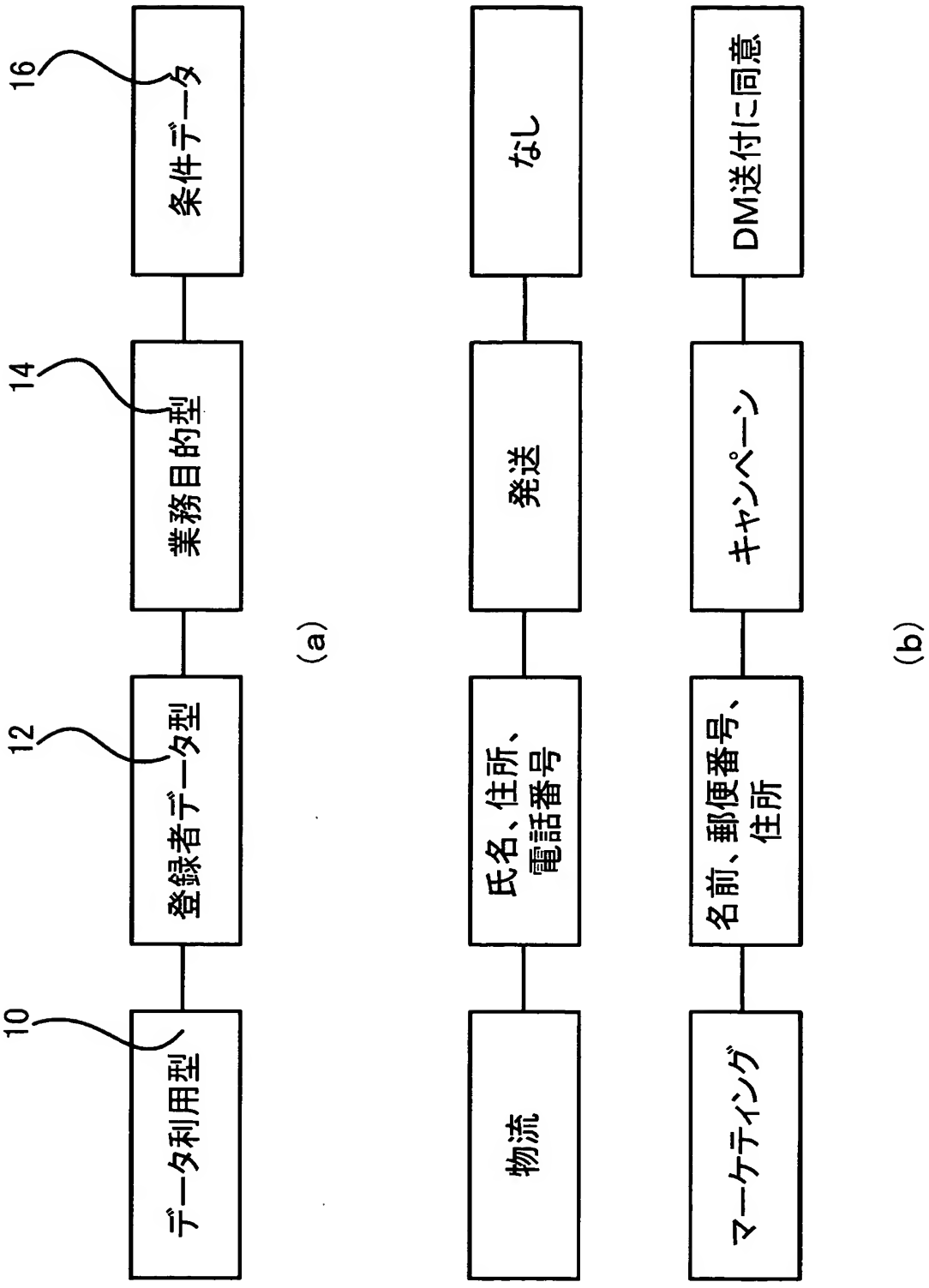
５２…ネットワーク

５４…アプリケーション・コンピュータ

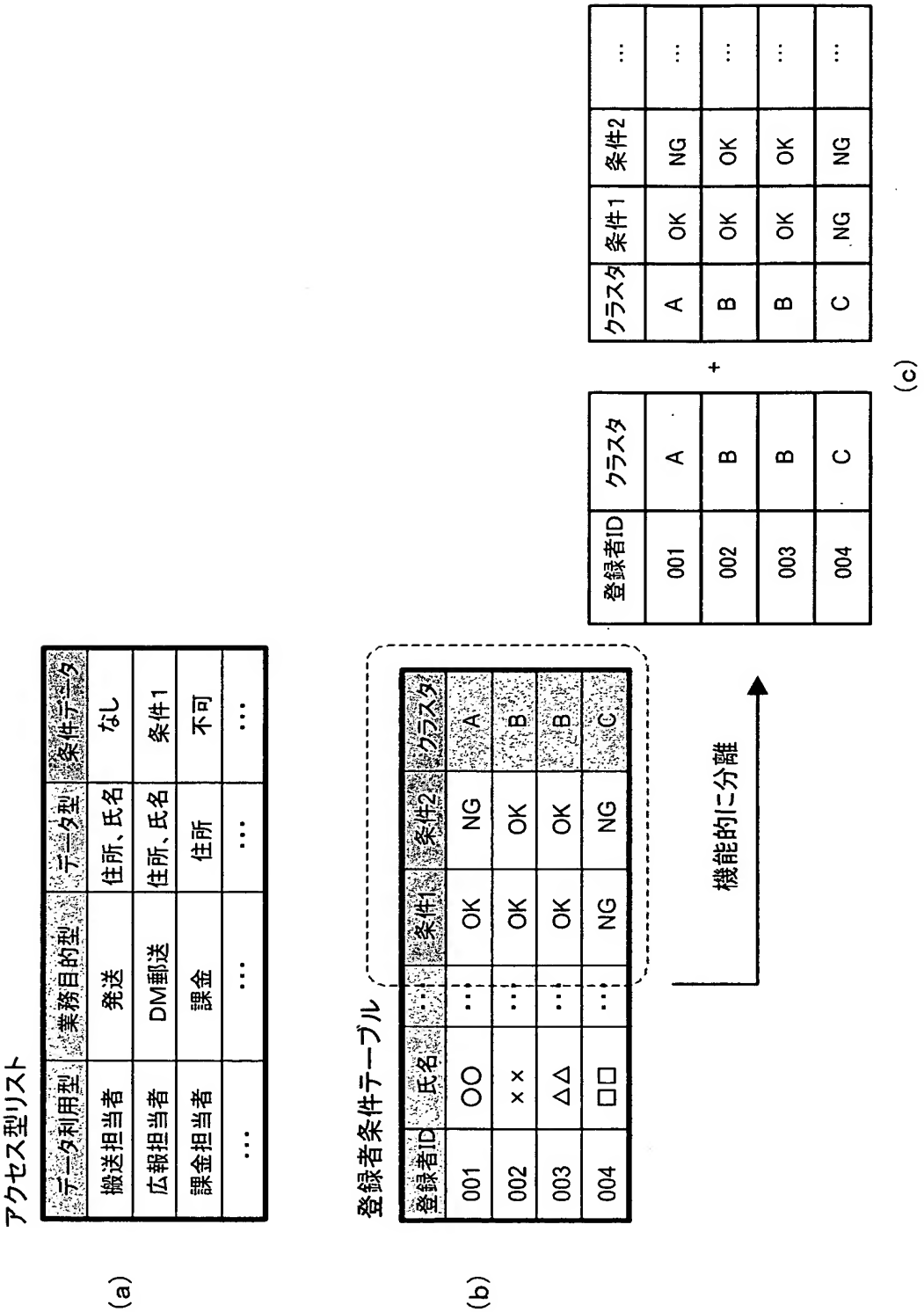
５６…管理サーバ

【書類名】　図面

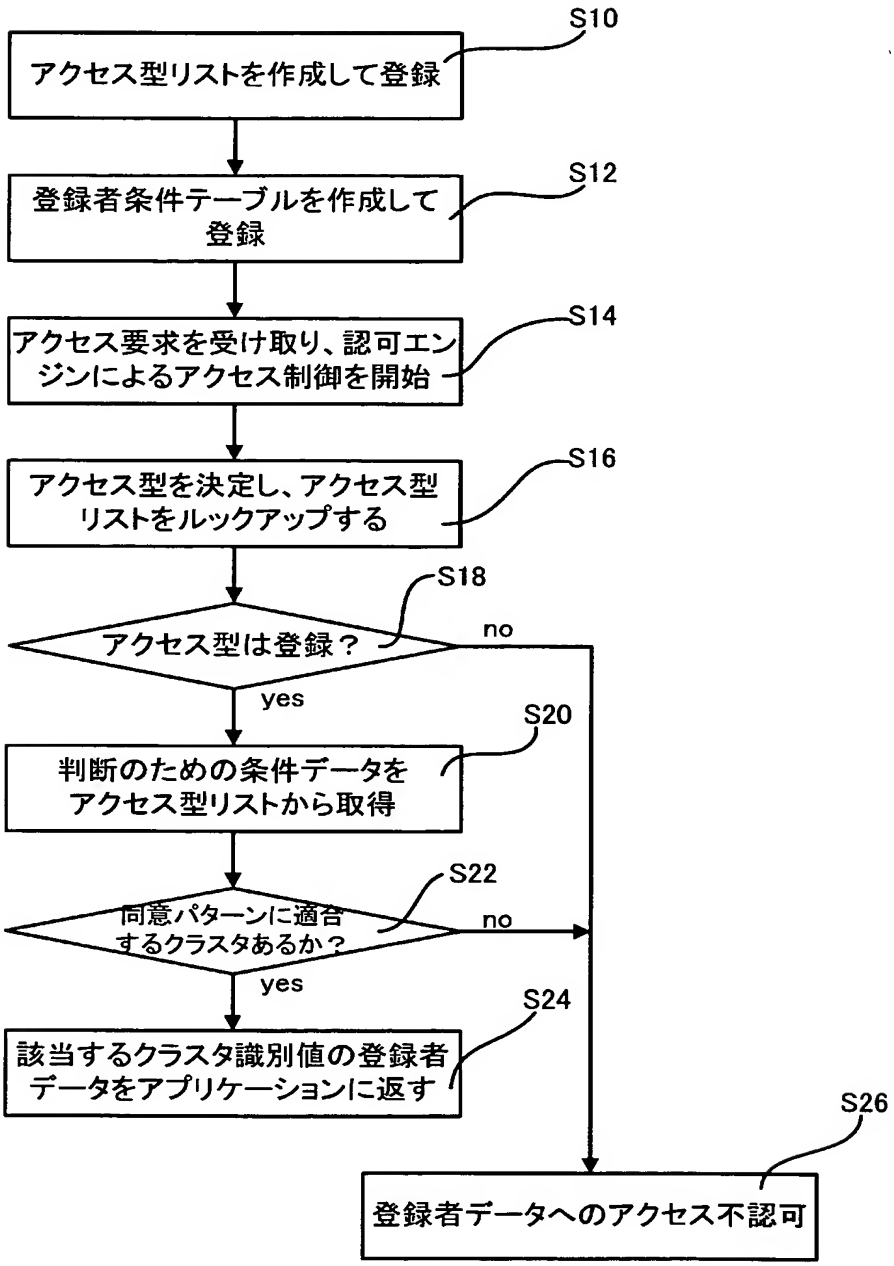
【図１】


10
データ利用型
12
登録者データ型
14
業務目的型
16
条件データ
(a)
物流
氏名、住所、
電話番号
発送
なし
(b)
マーケティング
名前、郵便番号、
住所
キャンペーン
DM送付に同意

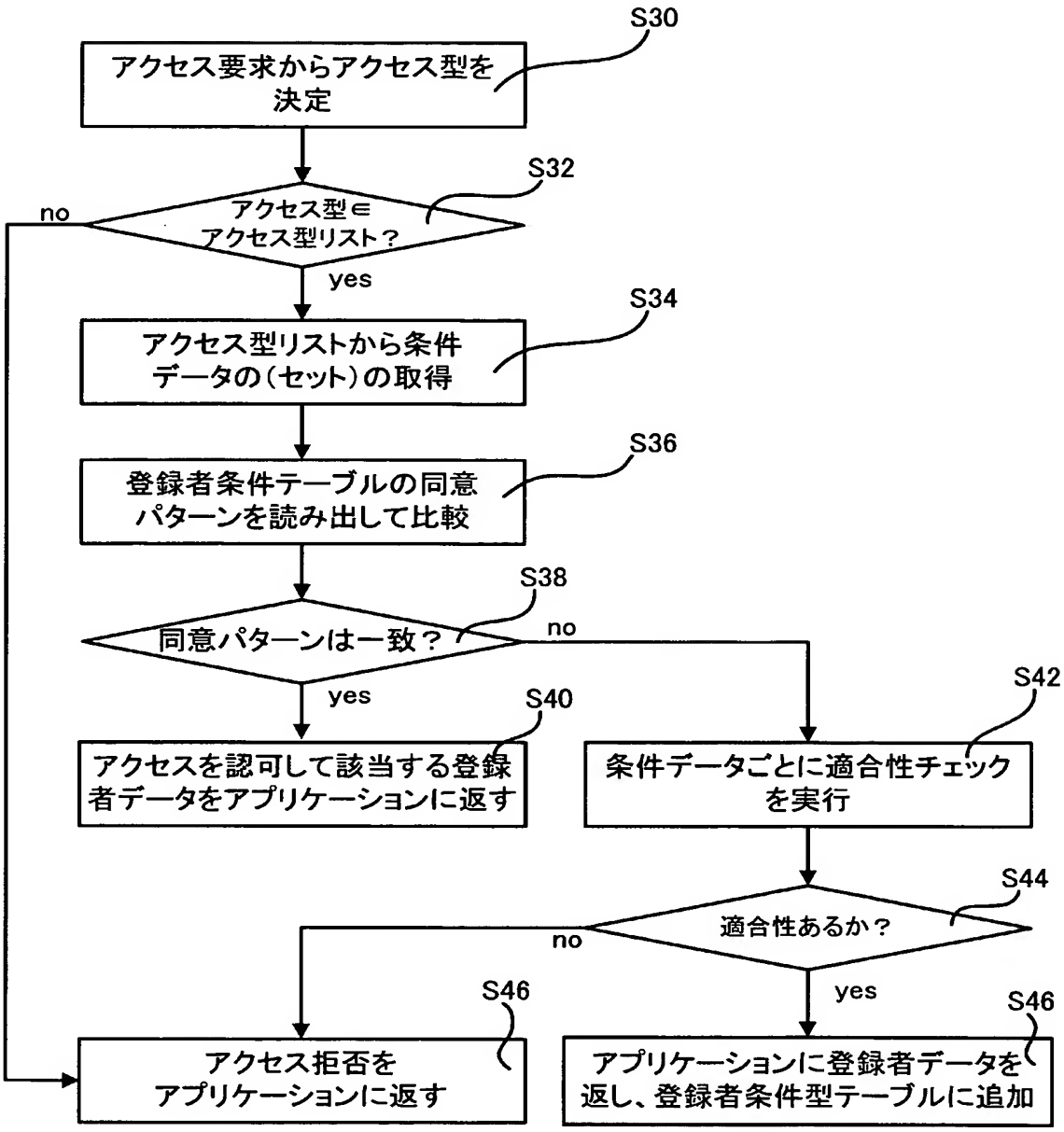
【図２】


アクセス型リスト
(a)
データ利用型
業務目的型
データ型
条件データ
搬送担当者
発送
住所、氏名
なし
広報担当者
DM郵送
住所、氏名
条件1
課金担当者
課金
住所
不可
…
…
…
…
(b)
登録者条件テーブル
登録者ID
氏名
…
条件1
条件2
クラスタ
001
OO
…
OK
NG
A
002
××
…
OK
OK
B
003
ΔΔ
…
OK
OK
B
004
□□
…
NG
NG
C
機能的に分離
登録者ID
クラスタ
001
A
002
B
003
B
004
C
+
クラスタ
条件1
条件2
A
OK
NG
B
OK
OK
B
OK
OK
C
NG
NG
(c)

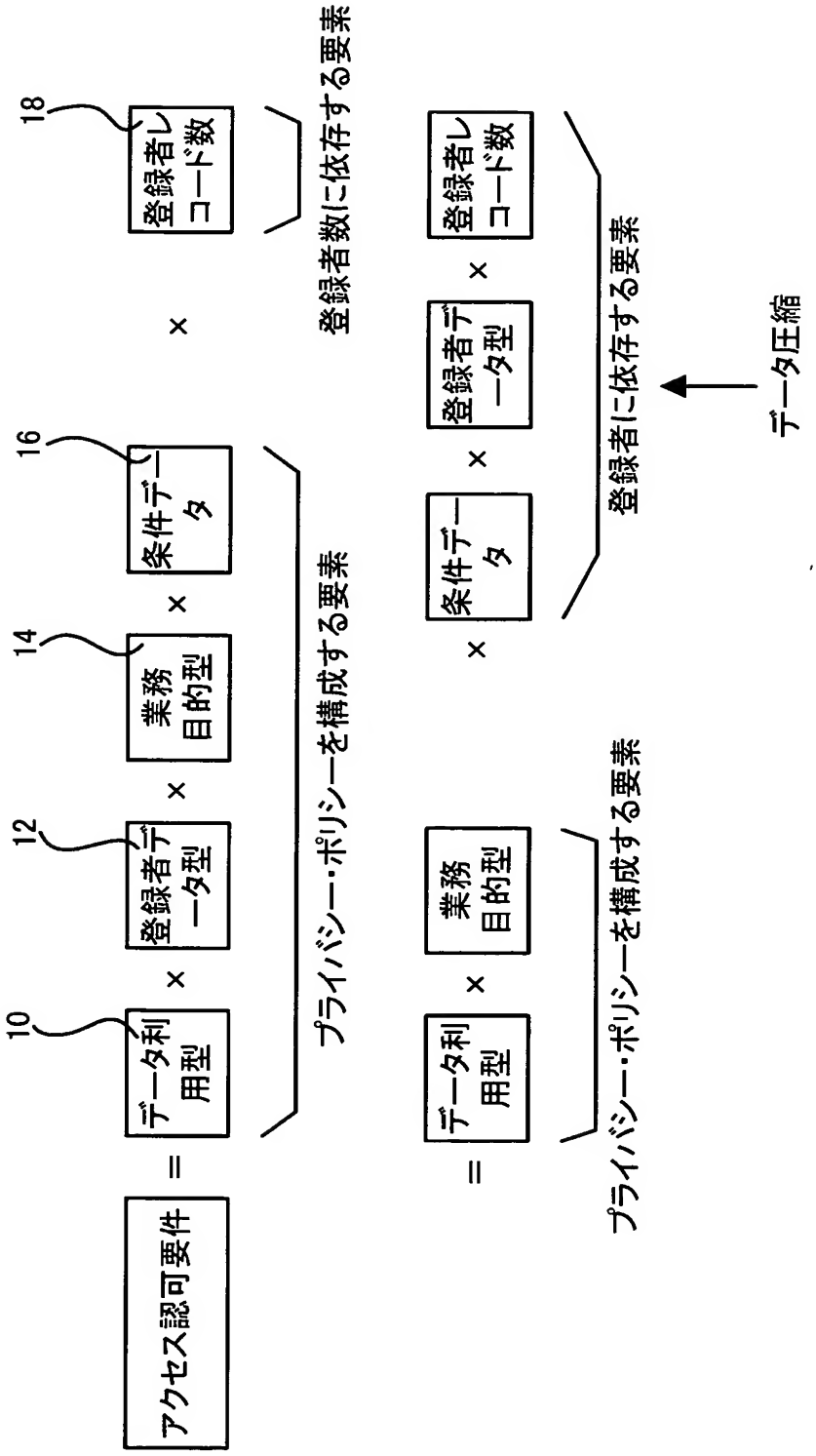
【図３】


S10
アクセス型リストを作成して登録
S12
登録者条件テーブルを作成して登録
S14
アクセス要求を受け取り、認可エンジンによるアクセス制御を開始
S16
アクセス型を決定し、アクセス型リストをルックアップする
S18
アクセス型は登録？
no
yes
S20
判断のための条件データをアクセス型リストから取得
S22
同意パターンに適合するクラスタあるか？
no
yes
S24
該当するクラスタ識別値の登録者データをアプリケーションに返す
S26
登録者データへのアクセス不認可

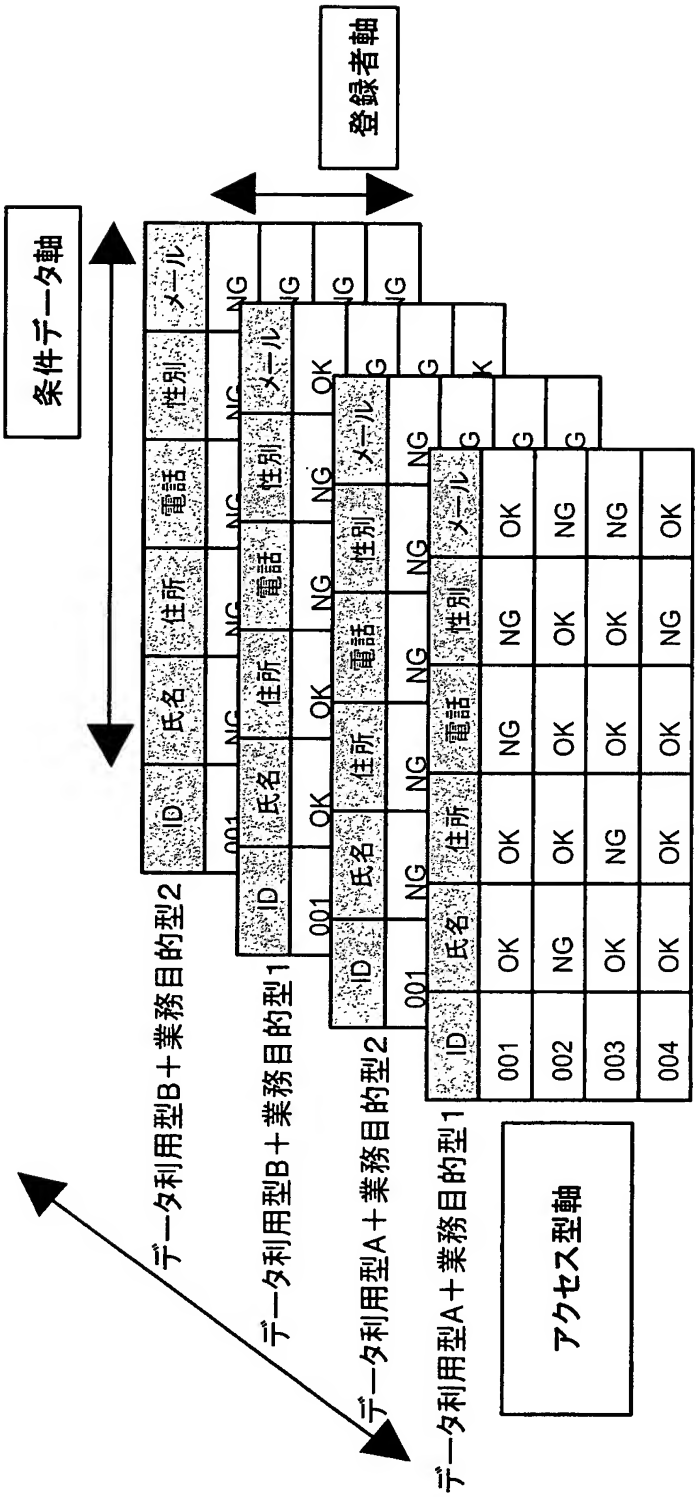
【図４】


S30
アクセス要求からアクセス型を決定
S32
アクセス型∈アクセス型リスト？
no
yes
S34
アクセス型リストから条件データの（セット）の取得
S36
登録者条件テーブルの同意パターンを読み出して比較
S38
同意パターンは一致？
no
yes
S40
アクセスを認可して該当する登録者データをアプリケーションに返す
S42
条件データごとに適合性チェックを実行
S44
適合性あるか？
no
yes
S46
アクセス拒否をアプリケーションに返す
S46
アプリケーションに登録者データを返し、登録者条件型テーブルに追加

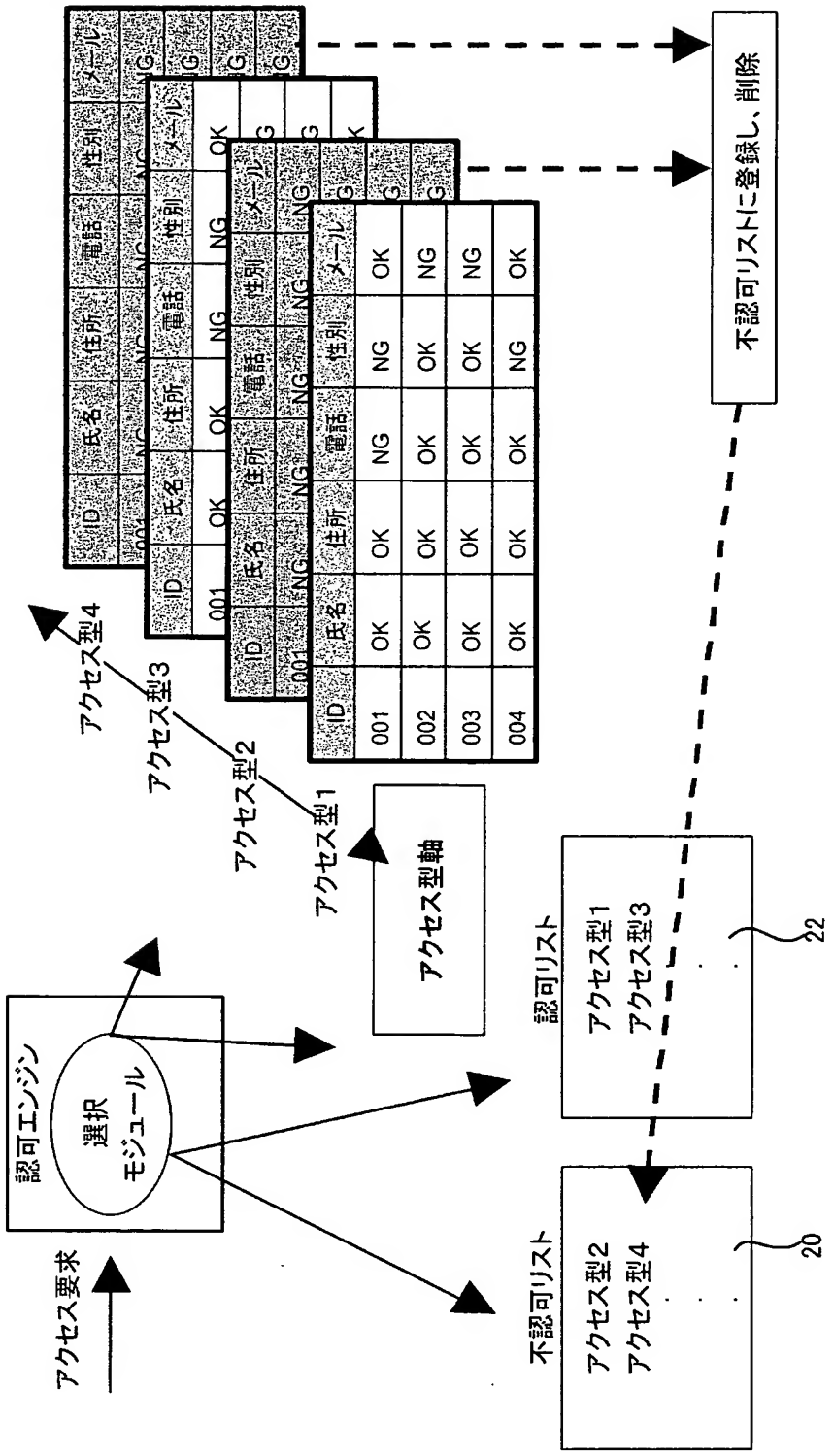
【図５】


アクセス認可要件
=
データ利用型
10
×
登録者データ型
12
×
業務目的型
14
×
条件データ
16
×
登録者レコード数
18
プライバシー・ポリシーを構成する要素
登録者数に依存する要素
=
データ利用型
×
業務目的型
プライバシー・ポリシーを構成する要素
×
条件データ
×
登録者データ型
×
登録者レコード数
登録者に依存する要素
データ圧縮

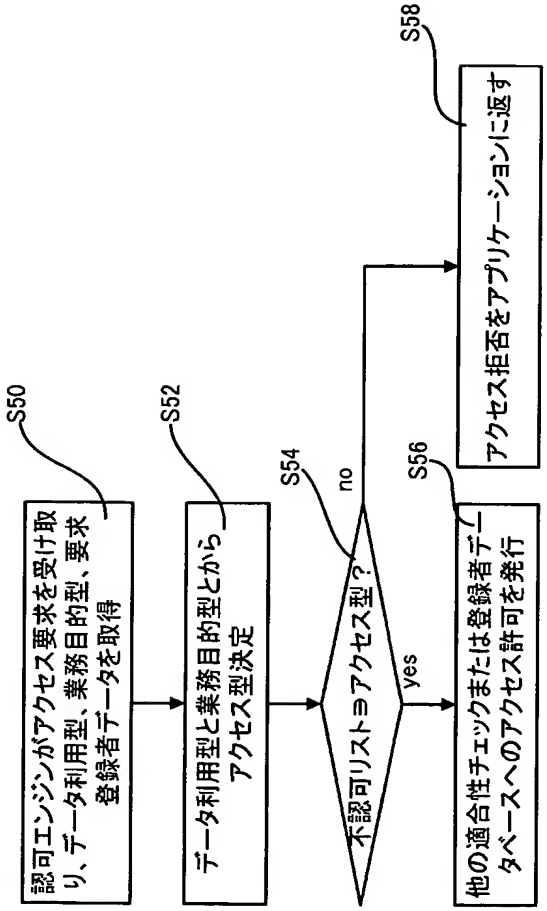
【図６】


登録者軸
条件データ軸
データ利用型B＋業務目的型2
データ利用型B＋業務目的型1
データ利用型A＋業務目的型2
データ利用型A＋業務目的型1
アクセス型軸
ID
氏名
住所
電話
性別
メール
001
OK
NG
002
003
004

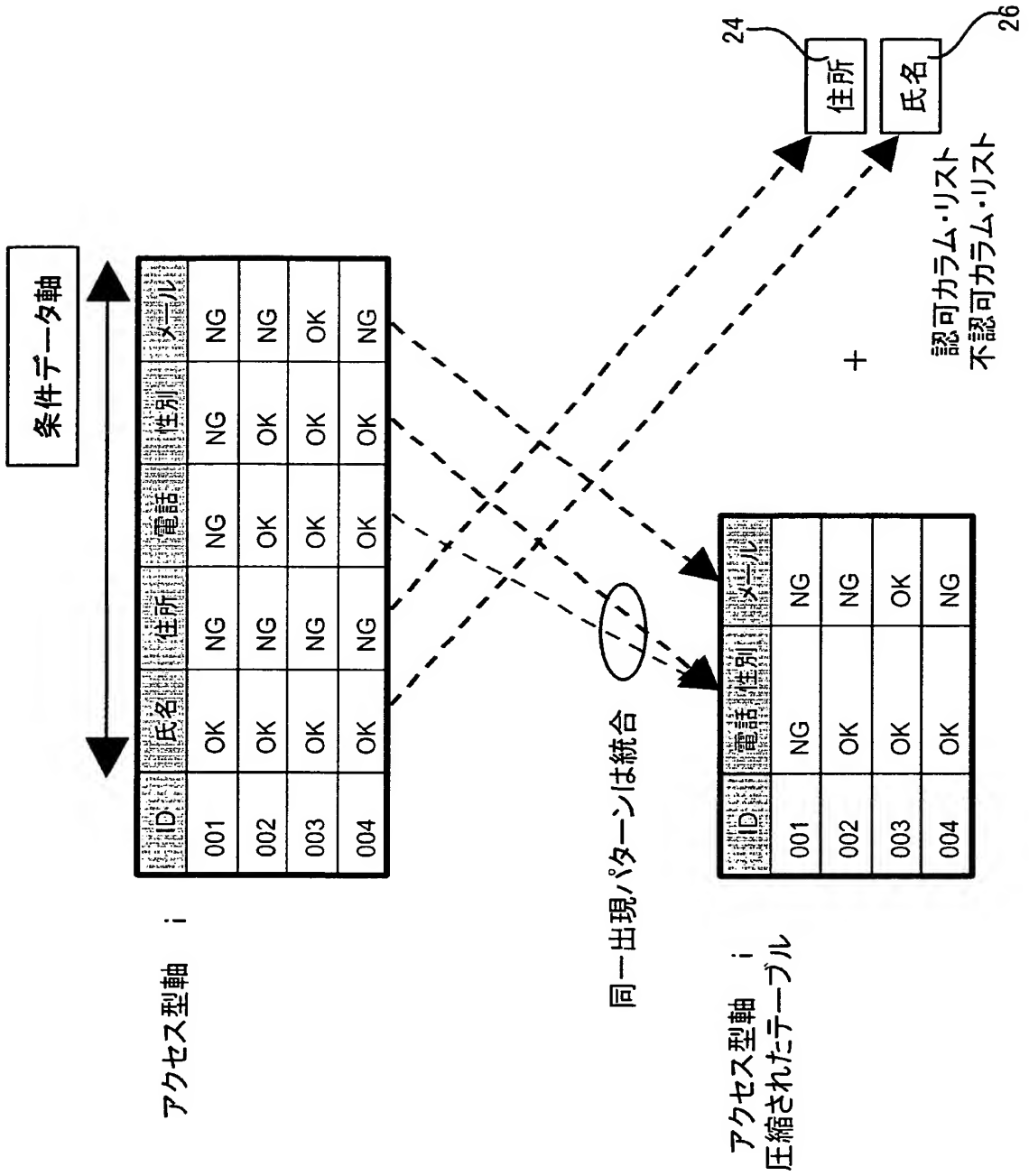
【図７】


アクセス要求
認可エンジン
選択モジュール
アクセス型軸
アクセス型4
アクセス型3
アクセス型2
アクセス型1
ID 氏名 住所 電話 性別 メール
001 OK OK OK NG OK
002 OK OK OK OK NG
003 OK OK OK OK NG
004 OK OK OK NG OK
不認可リスト
アクセス型2
アクセス型4
20
認可リスト
アクセス型1
アクセス型3
22
不認可リストに登録し、削除

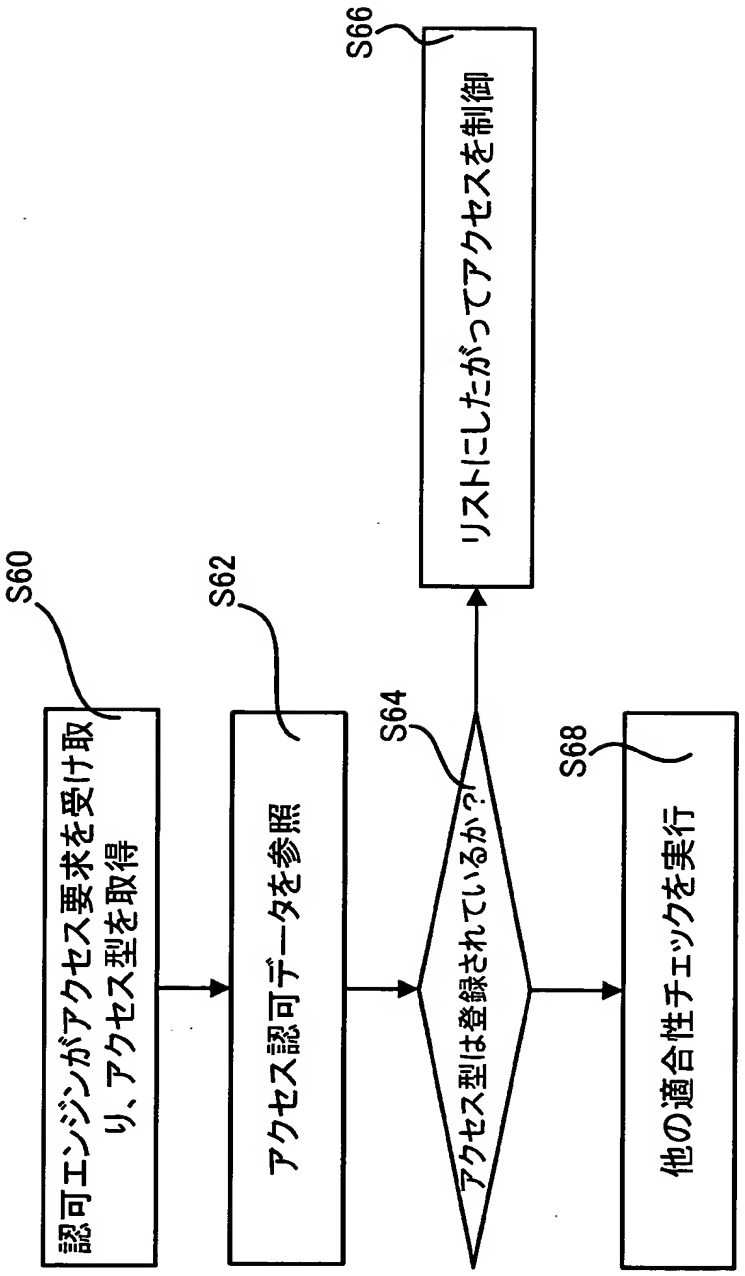
【図８】


S50
認可エンジンがアクセス要求を受け取り、データ利用型、業務目的型、要求登録者データを取得
S52
データ利用型と業務目的型とからアクセス型決定
S54
不認可リストヨアクセス型？
no
yes
S56
他の適合性チェックまたは登録者データベースへのアクセス許可を発行
S58
アクセス拒否をアプリケーションに返す

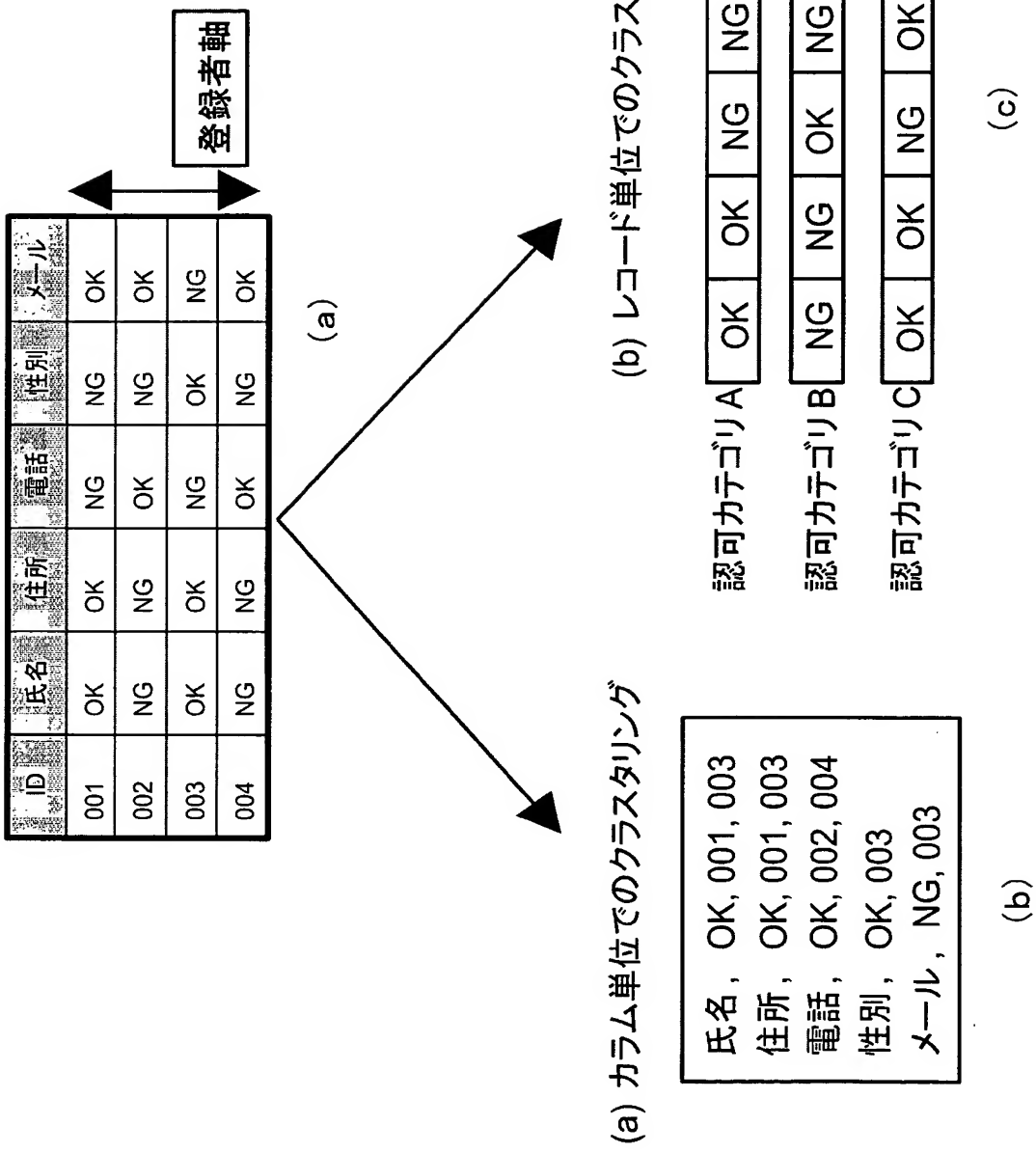
【図９】


条件データ軸
ID
氏名
住所
電話
性別
メール
001 OK NG NG NG NG
002 OK NG OK OK NG
003 OK NG OK OK OK
004 OK NG OK OK NG
アクセス型軸　i
同一出現パターンは統合
ID
電話
性別
メール
001 NG NG
002 OK NG
003 OK OK
004 OK NG
アクセス型軸　i
圧縮されたテーブル
24
住所
26
氏名
+
認可カラム・リスト
不認可カラム・リスト

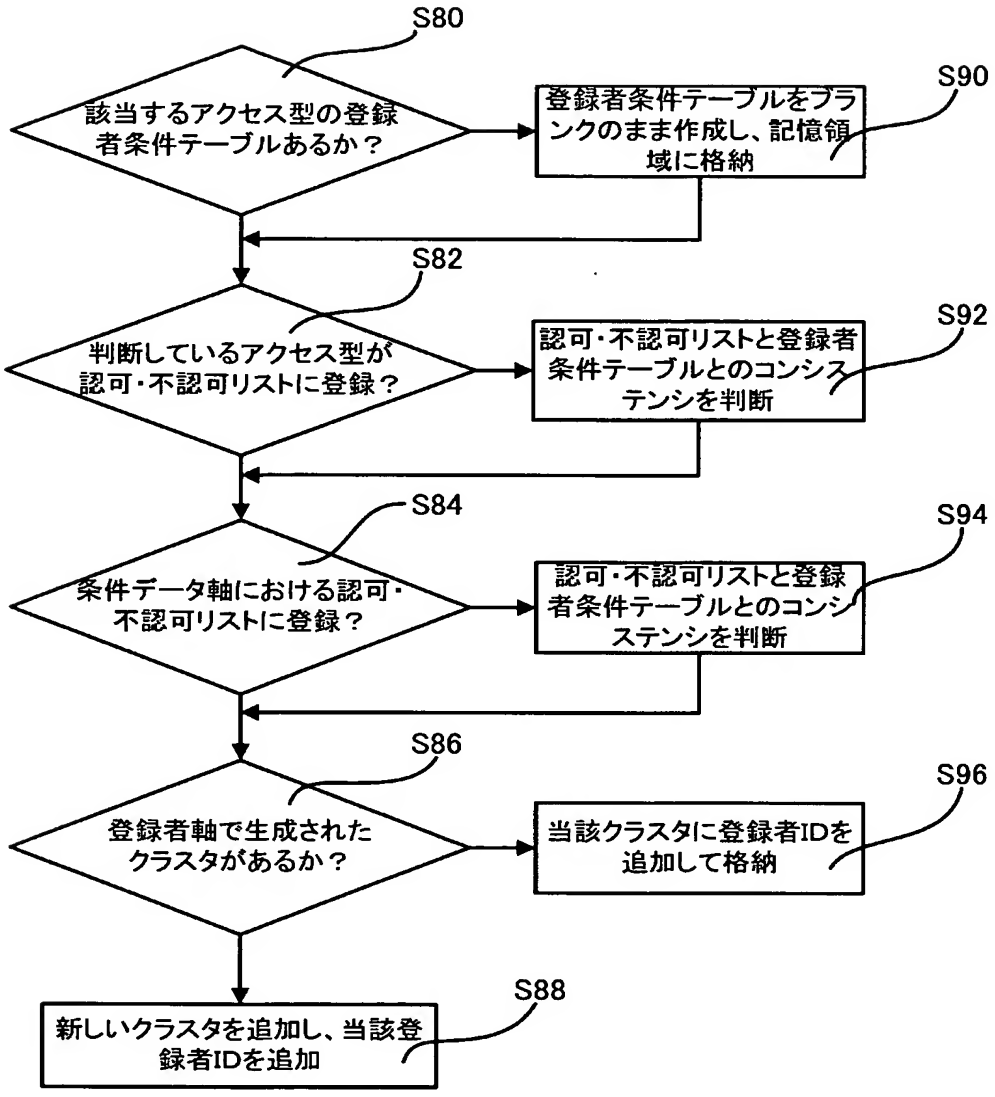
【図１０】


S60
認可エンジンがアクセス要求を受け取り、アクセス型を取得
S62
アクセス認可データを参照
S64
アクセス型は登録されているか？
S66
リストにしたがってアクセスを制御
S68
他の適合性チェックを実行

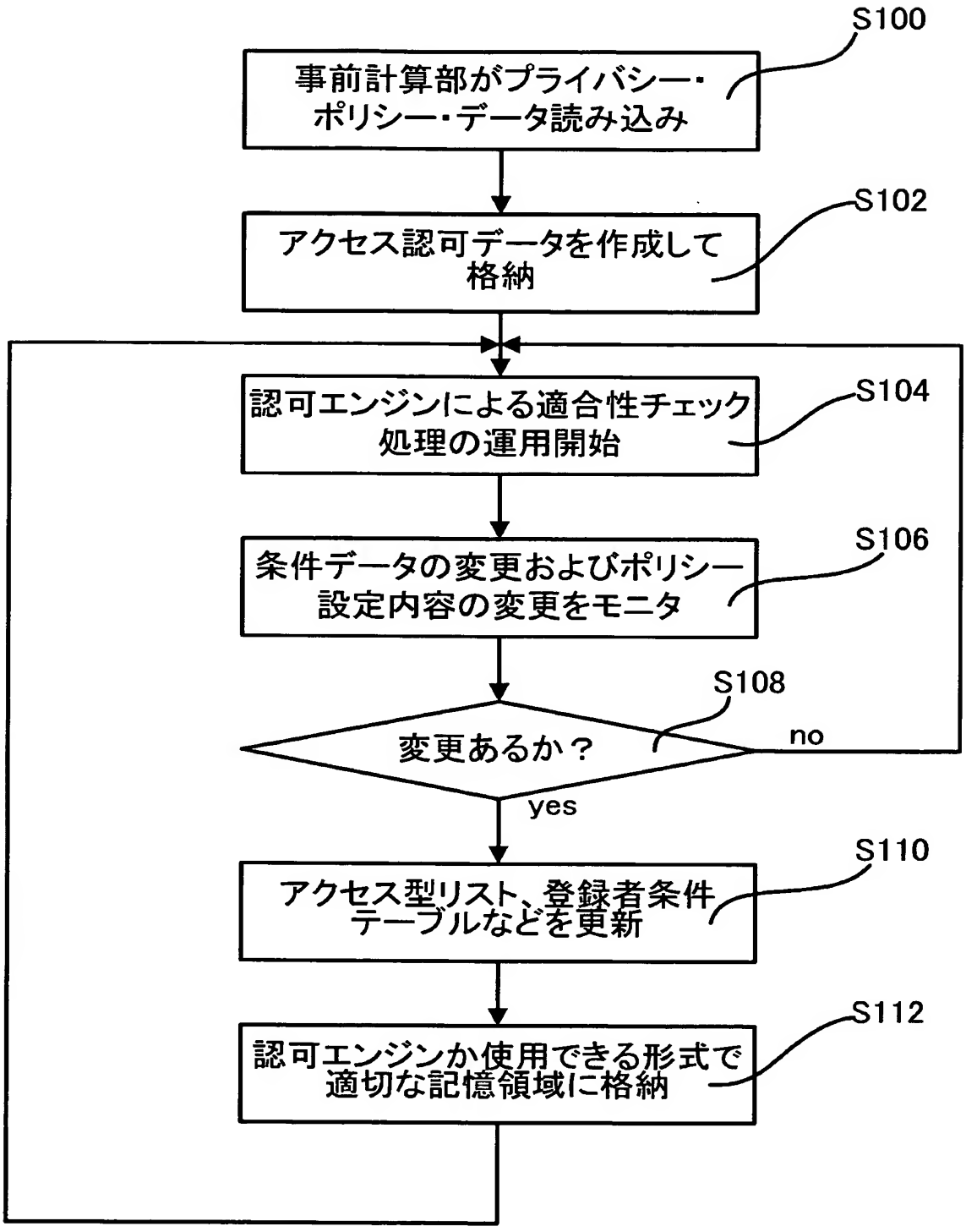
【図１１】


登録者軸
ID
氏名
住所
電話
性別
メール
001 OK OK NG NG OK
002 NG NG OK NG OK
003 OK OK NG OK OK
004 NG NG OK NG OK
(a)
(a) カラム単位でのクラスタリング
氏名，OK, 001, 003
住所，OK, 001, 003
電話，OK, 002, 004
性別，OK, 003
メール，NG, 003
(b)
(b) レコード単位でのクラスタリング
ID
認可カテゴリA OK OK NG NG OK 001
認可カテゴリB NG NG OK NG OK 002, 004
認可カテゴリC OK OK NG OK NG 003
(c)

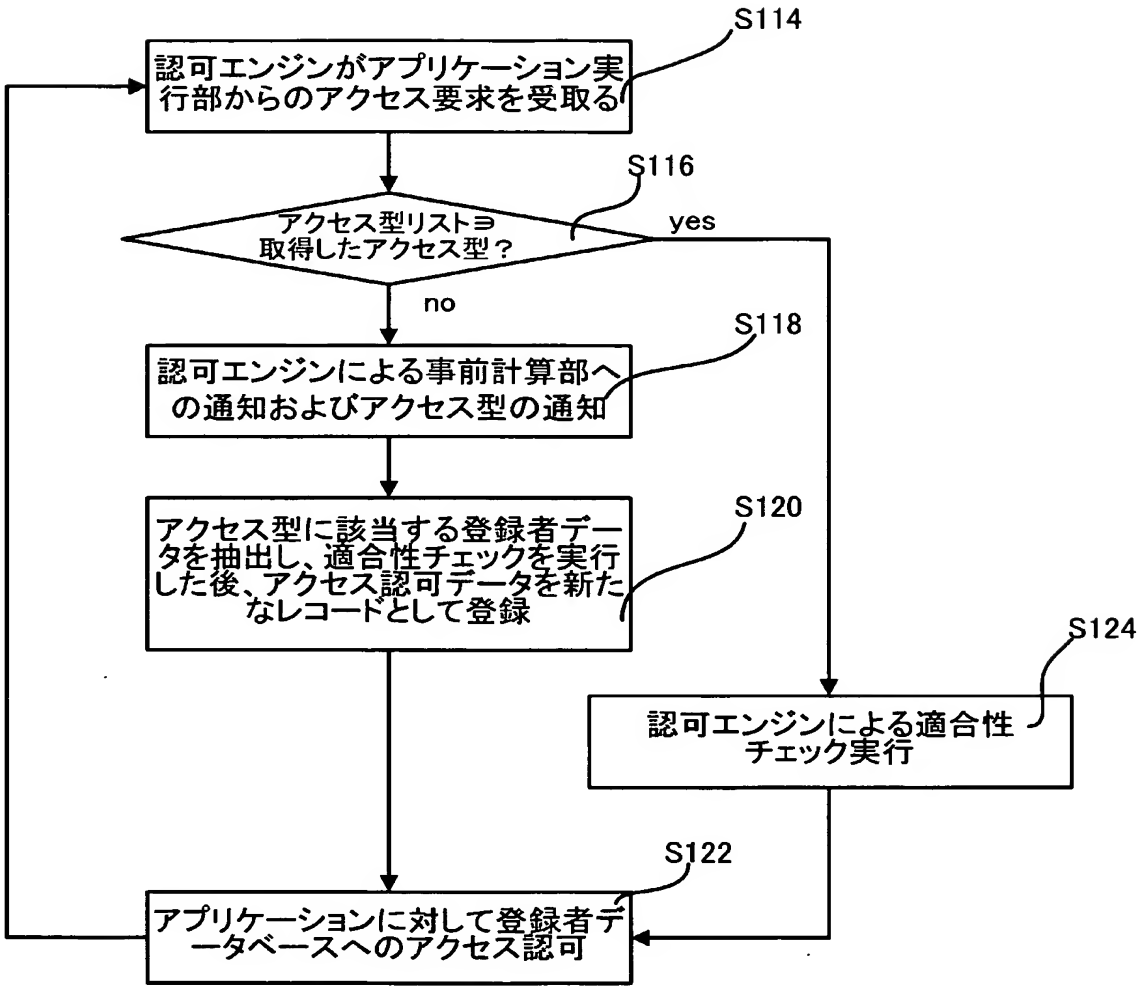
【図１２】


S80
該当するアクセス型の登録者条件テーブルあるか？
S90
登録者条件テーブルをブランクのまま作成し、記憶領域に格納
S82
判断しているアクセス型が認可・不認可リストに登録？
S92
認可・不認可リストと登録者条件テーブルとのコンシステンシを判断
S84
条件データ軸における認可・不認可リストに登録？
S94
認可・不認可リストと登録者条件テーブルとのコンシステンシを判断
S86
登録者軸で生成されたクラスタがあるか？
S96
当該クラスタに登録者IDを追加して格納
S88
新しいクラスタを追加し、当該登録者IDを追加

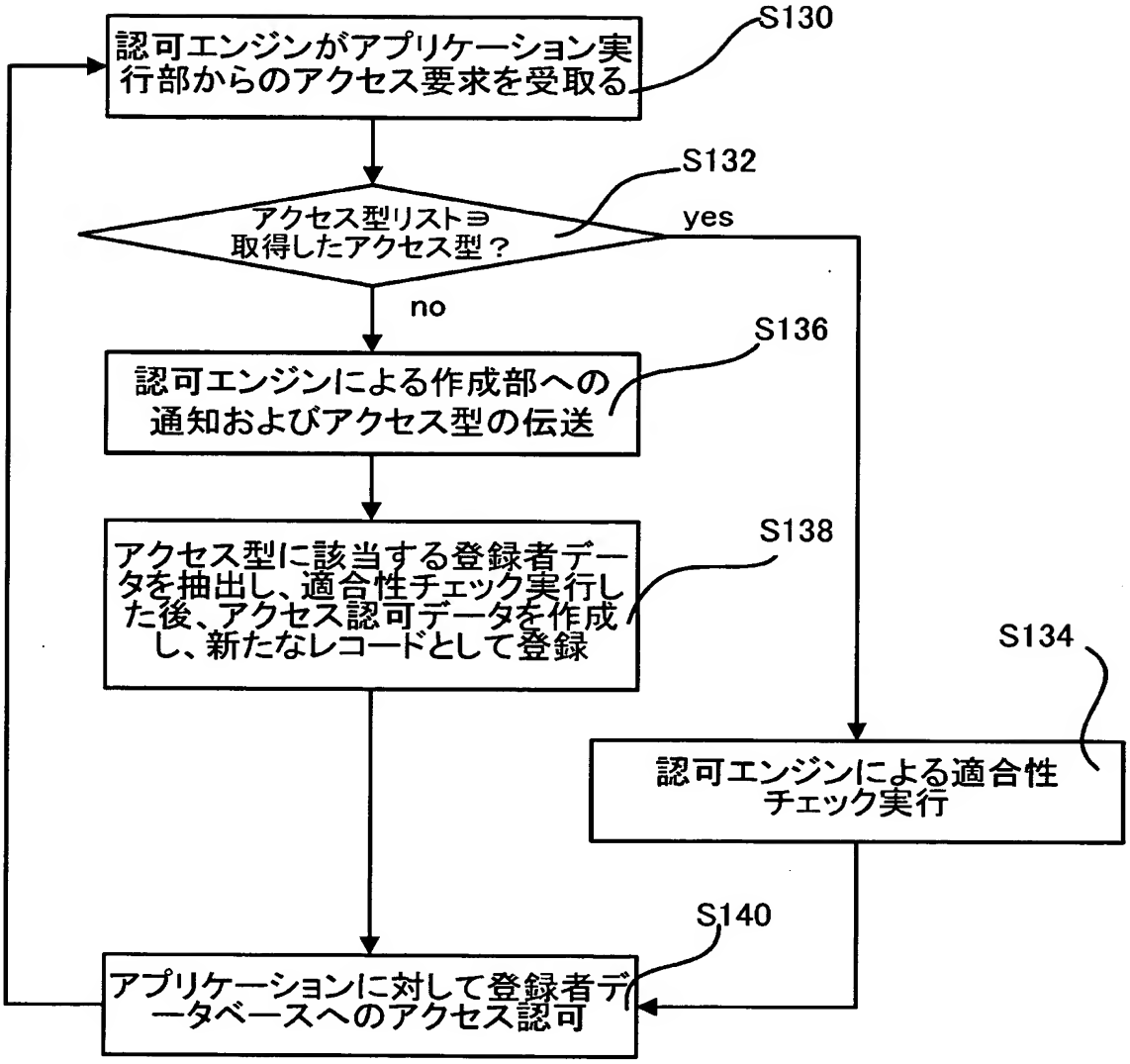
【図１３】


S100
事前計算部がプライバシー・ポリシー・データ読み込み
S102
アクセス認可データを作成して格納
S104
認可エンジンによる適合性チェック処理の運用開始
S106
条件データの変更およびポリシー設定内容の変更をモニタ
S108
変更あるか？
no
yes
S110
アクセス型リスト、登録者条件テーブルなどを更新
S112
認可エンジンか使用できる形式で適切な記憶領域に格納

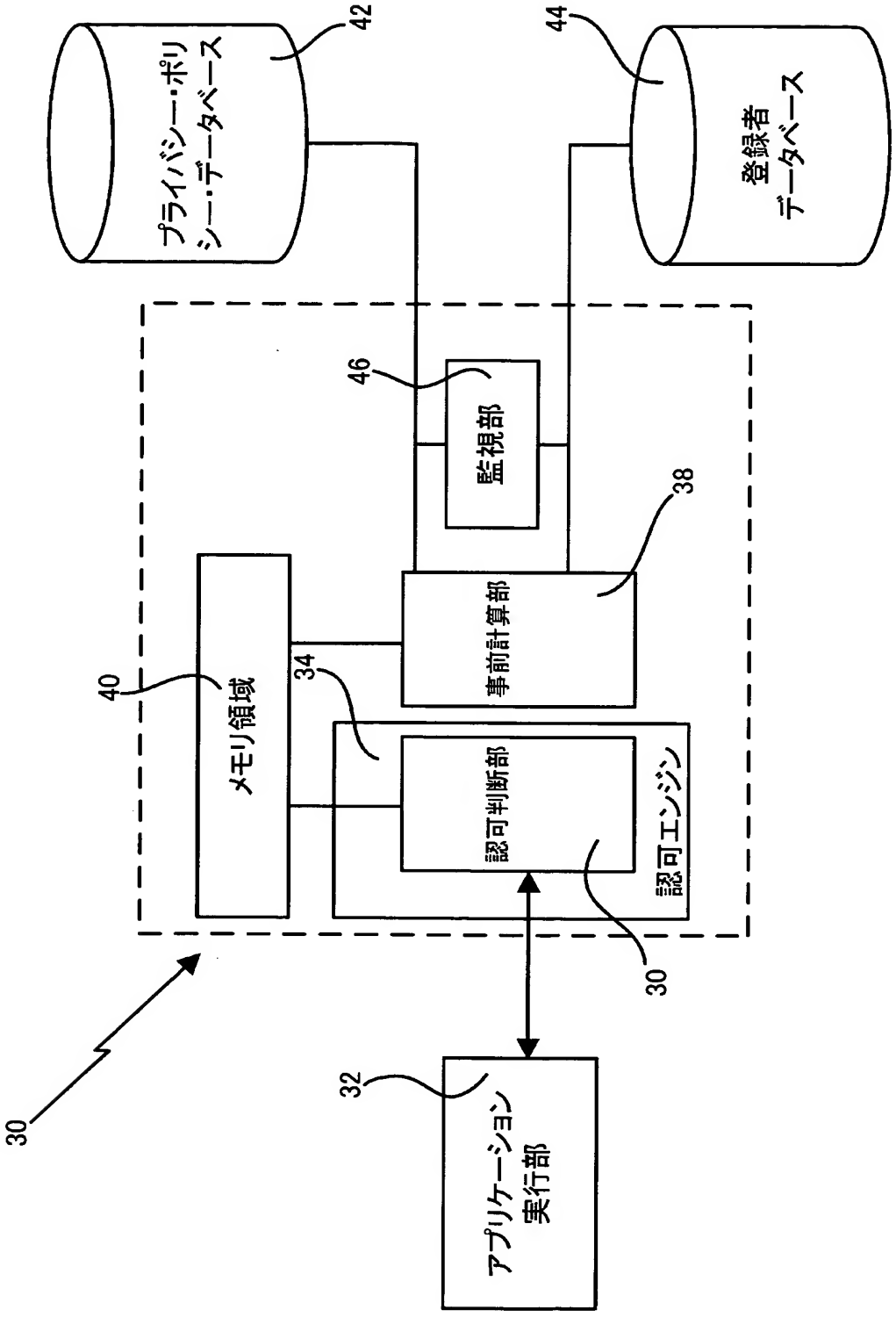
【図１４】


S114
認可エンジンがアプリケーション実行部からのアクセス要求を受取る
S116
アクセス型リスト∋取得したアクセス型？
yes
no
S118
認可エンジンによる事前計算部への通知およびアクセス型の通知
S120
アクセス型に該当する登録者データを抽出し、適合性チェックを実行した後、アクセス認可データを新たなレコードとして登録
S124
認可エンジンによる適合性チェック実行
S122
アプリケーションに対して登録者データベースへのアクセス認可

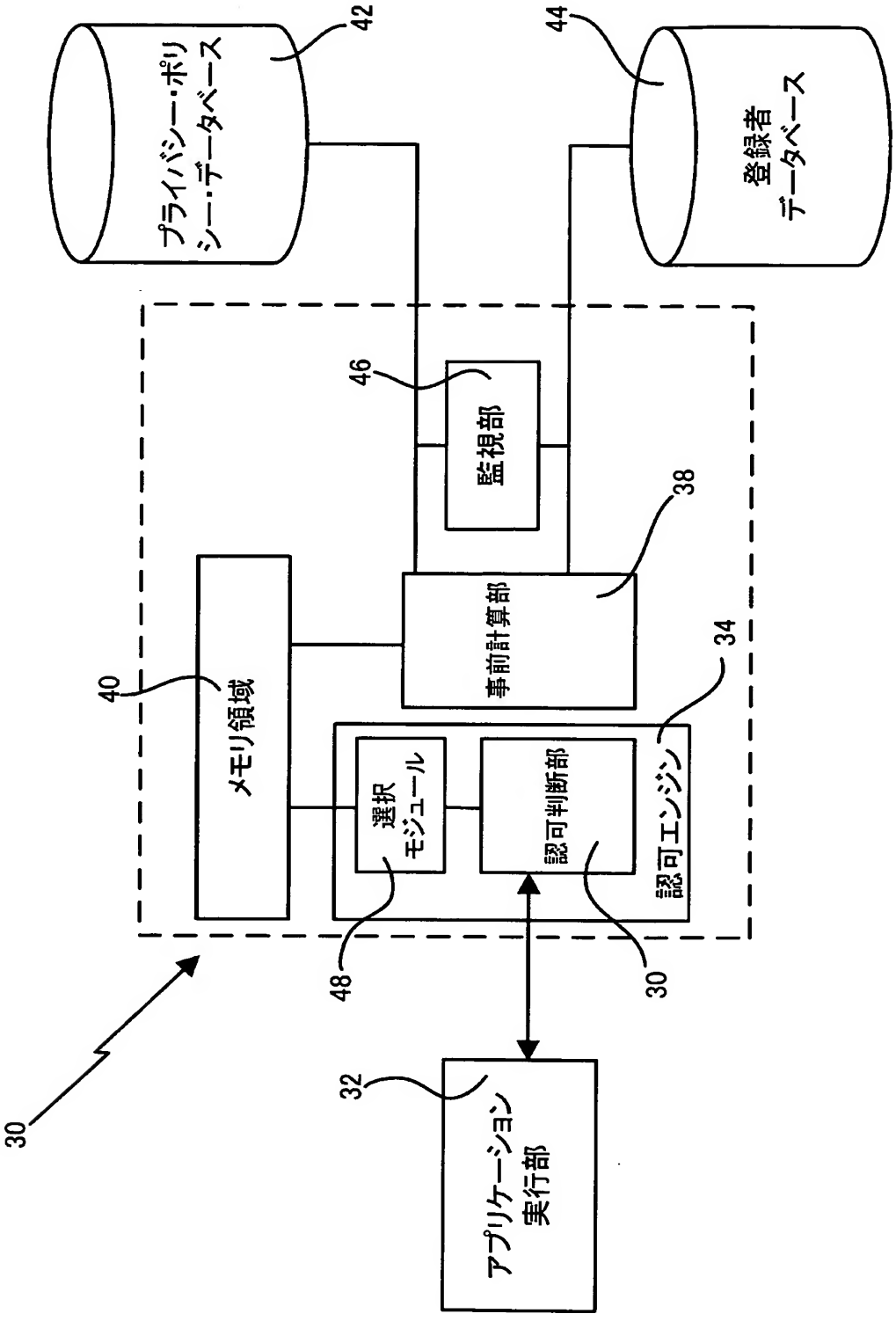
【図１５】


認可エンジンがアプリケーション実行部からのアクセス要求を受取る
S130
アクセス型リスト∋取得したアクセス型？
S132
yes
no
認可エンジンによる作成部への通知およびアクセス型の伝送
S136
アクセス型に該当する登録者データを抽出し、適合性チェック実行した後、アクセス認可データを作成し、新たなレコードとして登録
S138
認可エンジンによる適合性チェック実行
S134
アプリケーションに対して登録者データベースへのアクセス認可
S140

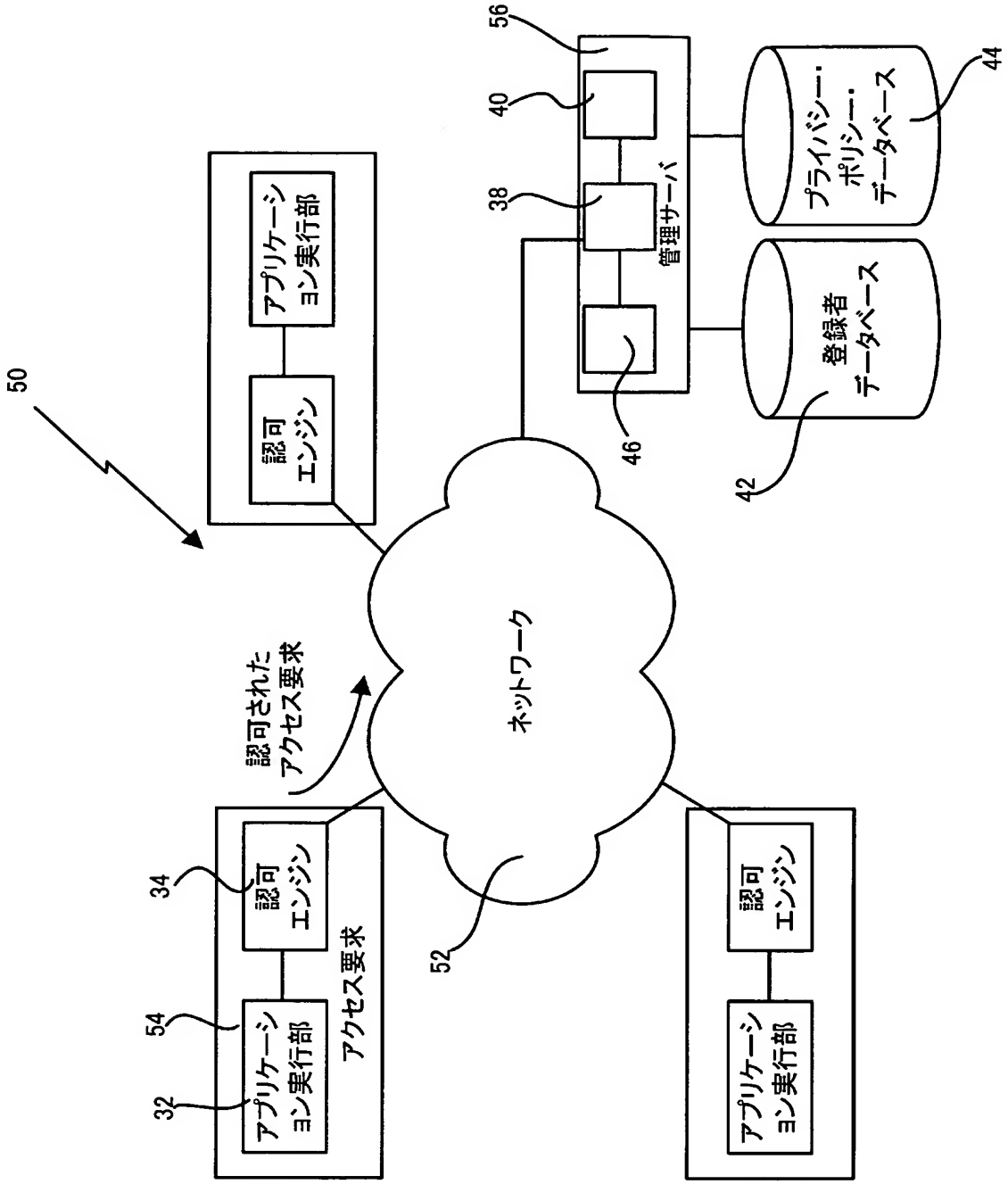
【図１６】


42
プライバシー・ポリシー・データベース
44
登録者データベース
46
監視部
38
事前計算部
40
メモリ領域
34
認可判断部
認可エンジン
30
30
32
アプリケーション実行部

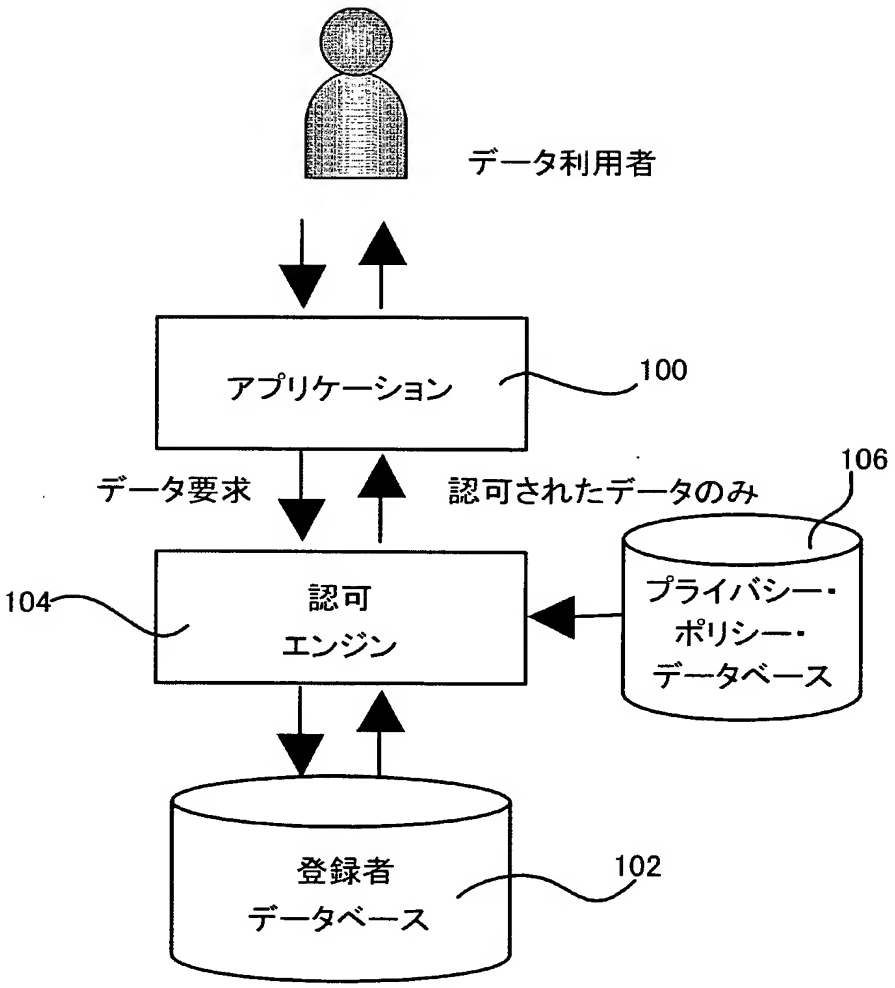
【図１７】


プライバシー・ポリシー・データベース
42
登録者データベース
44
監視部
46
事前計算部
38
メモリ領域
40
選択モジュール
認可判断部
認可エンジン
34
48
30
30
アプリケーション実行部
32

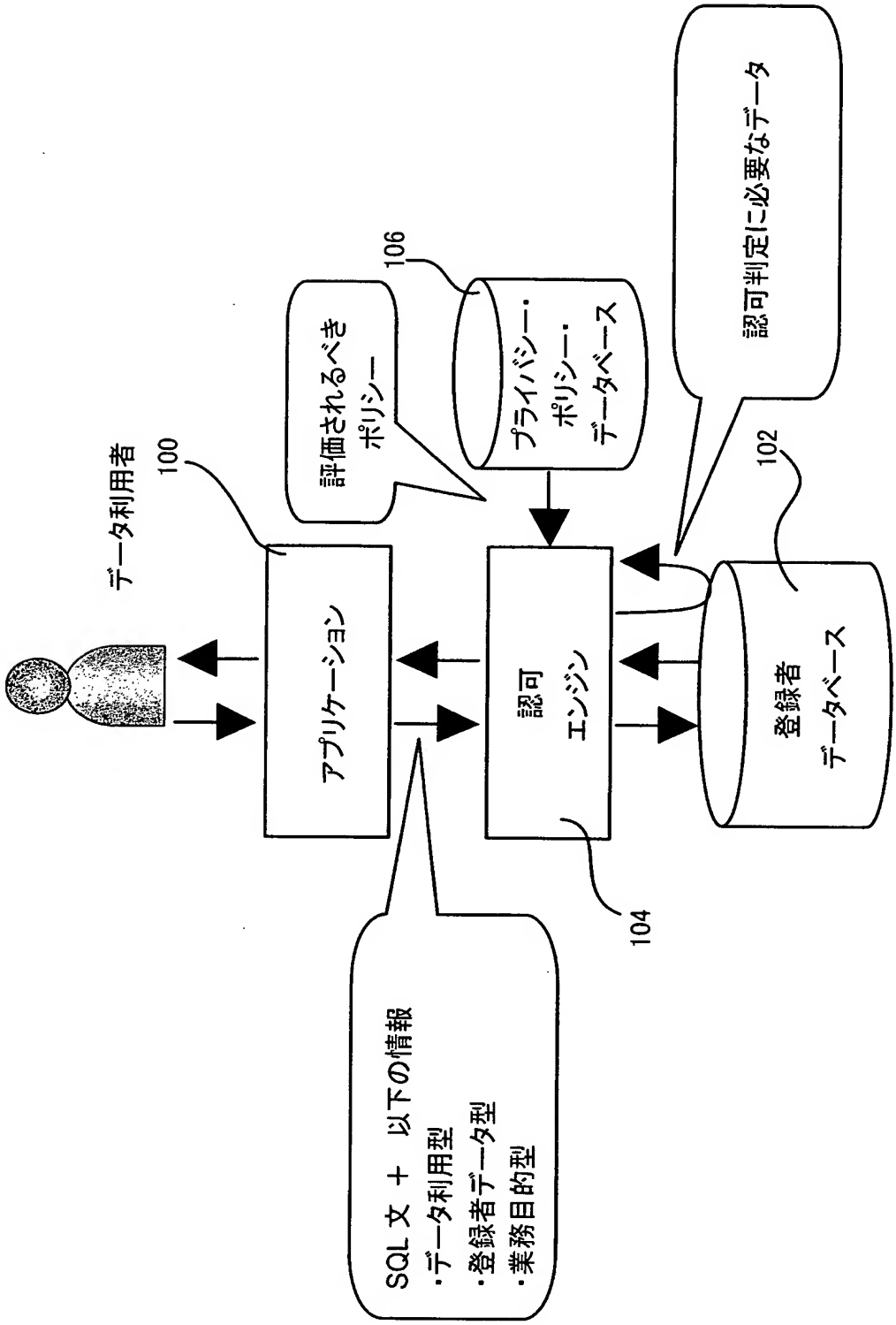
【図１８】


50
アプリケーション実行部
認可エンジン
56
40
38
管理サーバ
46
プライバシー・ポリシー・データベース
44
登録者データベース
42
ネットワーク
52
認可されたアクセス要求
34
認可エンジン
54
アプリケーション実行部
32
アクセス要求
認可エンジン
アプリケーション実行部

【図１９】


データ利用者
アプリケーション
100
データ要求
認可されたデータのみ
106
104
認可
エンジン
プライバシー・
ポリシー・
データベース
登録者
データベース
102

【図２０】


データ利用者
100
アプリケーション
評価されるべき
ポリシー
106
プライバシー・
ポリシー・
データベース
認可
エンジン
104
認可判定に必要なデータ
102
登録者
データベース
SQL 文 ＋ 以下の情報
・データ利用型
・登録者データ型
・業務目的型

【書類名】　要約書

【要約】

【課題】　アクセス管理システム、アクセス管理方法、該アクセス管理方法をコンピュータに実行させるためのコンピュータ実行可能なプログラムおよび該プログラムを記憶したコンピュータ可読な記憶媒体を提供する。

【解決手段】　本発明のアクセス管理システムは、登録者のプライバシー・データを含む登録者データを格納した登録者データベース４４へのアクセスを制御し、かつ、所定のプライバシー・ポリシーと登録者により指定された条件データとを使用して登録者データベース４４へのアクセスを制御する認可エンジン３４を含んでいる。認可エンジン３４は、外部から受信するアクセス要求からアクセス型を決定し、かつ登録者データについてアクセス型に関連してアクセス要求に先立って決定されるアクセス認可データを使用して、アクセス要求に基づく登録者データベースへの参照を制御する認可判断部３６を含んで構成されている。

【選択図】　図１６

認定・付加情報

特許出願の番号	特願２００３－０９０１３８
受付番号	５０３００５１３５８８
書類名	特許願
担当官	小野寺　光子　　１７２１
作成日	平成１５年　５月　８日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 390009531
- 【住所又は居所】 アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
- 【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【代理人】
- 【識別番号】 100108501
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社　知的所有権
- 【氏名又は名称】 上野　剛史

【復代理人】 申請人
- 【識別番号】 100110607
- 【住所又は居所】 神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山国際特許事務所
- 【氏名又は名称】 間山　進也

次頁無

特願２００３－０９０１３８

出　願　人　履　歴　情　報

識別番号　　［３９０００９５３１］

１．変更年月日　　２０００年　５月１６日
［変更理由］　　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション

２．変更年月日　　２００２年　６月　３日
［変更理由］　　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション